AFS

Guia do Usuário

Versão 3.6

G517-6974-00

AFS

Guia do Usuário

Versão 3.6

G517-6974-00

Nota

Antes de utilizar estas informações e o produto a que elas se referem, leia as informações gerais em "Avisos" na página 97.

Primeira Edição (Abril de 2000)

Esta edição aplica-se ao:

AFS para AIX, Versão 3.6
AFS para Digital Unix, Versão 3.6
AFS para HP-UX, Versão 3.6
AFS para Linux, Versão 3.6
AFS para SGI IRIX, Versão 3.6
AFS para Solaris, Versão 3.6

e a todos os releases e modificações posteriores até que indicado de outra forma em novas edições.

Solicite publicações através do seu representante IBM ou da filial da IBM que atende a sua localidade.

Índice

Sobre Este Manual

Esta seção descreve a finalidade, a organização e as convenções deste documento.

Público e Finalidade

Este manual descreve os conceitos e procedimentos para acesso às informações armazenadas no espaço de arquivo do AFS. Ele é destinado a usuários do AFS que estejam familiarizados com o UNIX mas não necessariamente com o AFS.

Este capítulo descreve os conceitos e diretrizes básicas para utilização do AFS e sintetiza algumas das diferenças entre os sistemas de arquivos do UNIX e o AFS. Os capítulos restantes explicam como executar funções básicas do AFS, como login, alteração de senhas, listagem de informações, proteção de arquivos, criação de grupos e detecção de problemas. Conceitos importantes para uma tarefa específica ou grupo específico de tarefas relacionadas são apresentados em contextos, exatamente antes dos procedimentos. Diversos exemplos são fornecidos.

As instruções geralmente contêm apenas os comandos e as opções de comandos necessárias para uma tarefa específica. Para obter uma lista completa dos comandos do AFS e a descrição de todas as opções disponíveis para cada comando, consulte o *AFS Administration Reference*.

Organização do Documento

Este documento está dividido nos seguintes capítulos.

O "Capítulo 1. Uma Introdução ao AFS" na página 1, apresenta os conceitos e funções básicas do AFS. Para ter sucesso na utilização do AFS, é importante que você esteja familiarizado com os termos e conceitos descritos neste capítulo.

O "Capítulo 2. Utilizando o AFS" na página 13, descreve como utilizar os recursos básicos do AFS: como efetuar o login e a autenticação, como desconectar-se, efetuar o logout, acessar arquivos e diretórios do AFS e como alterar sua senha.

O “Capítulo 3. Exibindo as Informações sobre o AFS” na página 25, descreve como exibir informações sobre a quota de volume e localização do AFS, o status da máquina servidor de arquivos e as células externas que você pode acessar.

O “Capítulo 4. Protegendo Seus Diretórios e Arquivos” na página 33, descreve como proteger seus dados utilizando as listas de controle de acesso (ACLs) do AFS.

O “Capítulo 5. Utilizando Grupos” na página 51, descreve como criar e gerenciar grupos.

O “Capítulo 6. Detecção de problemas” na página 67, descreve etapas detalhadas de diagnóstico e correção para problemas específicos.

O “Apêndice A. Utilizando o NFS/AFS Translator” na página 73, descreve como usar o NFS/AFS Translator para acessar o espaço de arquivo do AFS a partir de uma máquina cliente do NFS.

O “Apêndice B. Sintaxe do Comando e Ajuda Online AFS” na página 79, descreve a sintaxe de comandos do AFS e como obter informações online sobre os comandos.

O “Apêndice C. Glossário” na página 87, define os termos utilizados no *AFS User Guide*.

Como Utilizar Este Documento

Antes de começar a usar o AFS, leia o “Capítulo 1. Uma Introdução ao AFS” na página 1. Em seguida, siga os procedimentos apresentados no “Capítulo 2. Utilizando o AFS” na página 13, para começar a usar o AFS como um usuário autenticado. Ele descreve como acessar arquivos no espaço de arquivo do AFS e como encerrar uma sessão do AFS. Consulte os outros capítulos à medida que precisar executar as tarefas neles descritas.

Documentos Relacionados

O Kit de Documentações do AFS também contém os seguintes documentos:

- O *AFS Administration Reference* detalha a sintaxe de cada comando do AFS e é destinado ao administrador, programador ou usuário experiente do AFS. Para cada comando do AFS, o *AFS Administration Reference* relaciona a sintaxe do comando, os aliases e abreviações, a descrição, os argumentos, as advertências, os resultados de saída, os exemplos e os tópicos relacionados. Os comandos estão organizados em ordem alfabética.

- O *AFS Administration Guide* descreve os conceitos e procedimentos necessários para administração de uma célula do AFS, assim como uma maior cobertura dos tópicos do *AFS User Guide*.
- O *AFS Quick Beginnings* fornece as instruções para instalação das máquinas do servidor e do cliente do AFS.

Convenções Tipográficas

Este documento usa as seguintes convenções tipográficas:

- Os nomes de comandos e opções aparecem em **negrito** em definições de sintaxe, exemplos e textos em execução. Os nomes dos diretórios, arquivos, máquinas, partições, volumes e usuários também aparecem em **negrito**.
- As informações variáveis aparecem em *itálico*. Elas incluem informações fornecidas pelo usuário em linhas de comandos e as partes dos prompts que diferem dependendo de quem emite o comando. Os termos novos também aparecem em *itálico*.
- Os exemplos de saídas de tela e conteúdo de arquivos aparecem em `mono espaço`.

Além disso, estes símbolos aparecem nas definições da sintaxe do comando, tanto na documentação, quanto nas instruções da ajuda online do AFS. Ao emitir um comando, não digite estes símbolos.

- Os colchetes **[ ]** são colocados em itens opcionais.
- Os sinais de maior ou menor (**< >**) são colocados nos valores fornecidos pelo usuário em comandos AFS.
- Um sinal de mais sobrescrito **+** vem depois de um argumento que aceita mais do que um valor.
- O sinal de porcentagem `%` representa o prompt do shell do comando regular. Alguns sistemas operacionais possivelmente usam um caractere diferente para esse prompt.
- O sinal que indica número `#` representa o prompt do shell de comando da **raiz** do superusuário local. Alguns sistemas operacionais possivelmente usam um caractere diferente para esse prompt.
- O símbolo de canalização **|** em uma instrução da sintaxe do comando separa valores mutuamente exclusivos de um argumento.

Para obter outras informações sobre os comandos do AFS, incluindo descrições dos componentes da cadeia de comandos, abreviações e aliases aceitáveis e como obter ajuda online para os comandos, consulte “Apêndice B. Sintaxe do Comando e Ajuda Online AFS” na página 79.

Capítulo 1. Uma Introdução ao AFS

Este capítulo introduz os conceitos e termos básicos do AFS. Assumindo que você já esteja familiarizado com os comandos padrão do UNIX, com proteção de arquivos e com convenções de nomes de caminhos.

Conceitos do AFS

O AFS torna fácil o trabalho conjunto de pessoas em arquivos iguais, independente da localização dos arquivos. Os usuários do AFS não precisam saber em que máquina o arquivo está armazenado, e os administradores podem transferir arquivos entre as máquinas sem interromper o acesso do usuário. Os usuários sempre identificam um arquivo pelo mesmo nome de caminho, e o AFS encontra o arquivo correto automaticamente, assim como acontece no sistema de arquivos local em uma única máquina. Ao tornar fácil o compartilhamento de arquivos, o AFS não compromete a segurança dos arquivos compartilhados. Ele fornece um esquema sofisticado de segurança.

Computação de Cliente/Servidor

O AFS utiliza um modelo *de computação de cliente/servidor*. Na computação de cliente/servidor, há dois tipos de máquinas. *As máquinas do servidor* armazenam dados e executam serviços para máquinas do cliente. As *máquinas do cliente* realizam a computação para usuários e acessam dados e serviços fornecidos por máquinas do servidor. Algumas máquinas agem como clientes e servidores. Na maioria dos casos, você trabalha em uma máquina cliente, acessando os arquivos armazenados em uma máquina servidor de arquivos.

Sistemas de Arquivos Distribuídos

O AFS é um *sistema de arquivos distribuído* que une os sistemas de arquivos de várias máquinas de servidor de arquivos. Ele torna o acesso a arquivos armazenados em uma máquina de servidor de arquivos remota tão fácil como o acesso a arquivos armazenados no disco local. O sistema de arquivos distribuído tem duas principais vantagens em relação ao sistema de arquivos centralizado convencional:

- Disponibilidade ampliada: Uma cópia de um arquivo comum, como o binário de um programa de aplicação, pode ser armazenada em várias máquinas de servidor. Um período de inatividade em uma única máquina ou até mesmo em várias máquinas não torna necessariamente o arquivo indisponível. Ao invés disso, as solicitações de programa que o usuário faz são encaminhadas para máquinas acessíveis. Em um sistema de arquivos centralizado, a perda da máquina central de armazenamento do arquivo encerra efetivamente o sistema inteiro.

- Eficiência ampliada: Em um sistema de arquivos distribuído, a carga de trabalho é distribuída entre várias máquinas, que são servidores de arquivos menores. Elas apresentam uma tendência a ser mais amplamente utilizadas do que as máquinas maiores (e geralmente mais dispendiosas) de armazenamento em um sistema de arquivos centralizado.

O AFS oculta sua natureza distribuída, por isso ao trabalhar com arquivos do AFS temos a sensação de estar trabalhando com arquivos armazenados em uma máquina local, exceto pelo fato de se poder acessar mais arquivos. E como o AFS conta com a capacidade das máquinas do cliente para a computação, o aumento no número de usuários do AFS não torna consideravelmente lento o desempenho deste, transformando-o em um ambiente de computação muito eficiente.

Espaço de Arquivo do AFS e Espaço de Arquivo Local

O AFS atua como uma extensão do sistema de arquivos UNIX local de sua máquina. O administrador do sistema cria um diretório no disco local de cada máquina cliente do AFS para agir como um gateway para o AFS. Por convenção, este diretório é chamado de **/afs** e funciona como a raiz do *espaço de arquivo do AFS*.

Exatamente como o sistema de arquivos do UNIX, o AFS utiliza uma estrutura de arquivos hierárquica (uma árvore). Sob o diretório raiz **/afs** estão os subdiretórios criados pelo seu administrador do sistema, incluindo seu diretório de origem. Outros diretórios que encontram-se no mesmo nível do sistema de arquivos local que o **/afs**, como **/usr**, **/etc** ou **/bin**, podem estar localizados em seu disco local ou podem ser links para diretórios do AFS. Os arquivos relevantes apenas à máquina local são geralmente armazenados na máquina local. Todos os outros arquivos podem ser armazenados no AFS, permitindo que vários usuários os compartilhem e liberando o espaço em disco da máquina local para outros usuários.

Nota: Os comandos do AFS só podem ser usados em arquivos no espaço de arquivo deste ou nos diretórios locais que são links para o espaço de arquivo do AFS.

Células e Sites

A *célula* é o domínio administrativo no AFS. Os administradores de cada célula determinam como as máquinas do cliente são configuradas e o espaço de armazenamento disponível para cada usuário. A organização correspondente a uma célula pode ser uma empresa, o departamento de uma universidade ou qualquer grupo definido de usuários. Da perspectiva de um hardware, uma célula é um agrupamento de máquinas do cliente e de máquinas do servidor definidas para pertencer à mesma célula. Um *site* do AFS é um agrupamento de uma ou mais células relacionadas. Por exemplo, as células na Corporação ABC formam um único site.

Por convenção, os subdiretórios do diretório **/afs** são espaços de arquivo de células, cada um contendo subdiretórios e arquivos que pertencem a uma única célula. Por exemplo, os diretórios e arquivos relevantes à célula da Corporação ABC são armazenados no subdiretório **/afs/abc.com**.

Ao passo que cada célula organiza e mantém seu próprio espaço de arquivo, ela também pode conectar-se com o espaço de arquivo de outras células do AFS. O resultado é um espaço de arquivo enorme que possibilita o compartilhamento de arquivos dentro e entre as células.

A célula destinada à sua máquina cliente é chamada de sua *célula local*. Todas as outras células no espaço de arquivo do AFS são chamadas de *células externas*.

Volumes e Pontos de Instalação

Os discos de armazenamento em um computador são divididos em seções chamadas de *partições*. Além disso, o AFS divide as partições em unidades chamadas de *volumes* e cada um destes abriga uma subárvore de arquivos e diretórios relacionados. O volume fornece um container conveniente para o armazenamento de arquivos de diretórios relacionados. Os administradores do sistema podem transferir volumes de uma máquina servidor de arquivos para outra sem perceber, pois o AFS rastreia automaticamente a localização de um volume.

Você acessa o conteúdo de um volume acessando seu *ponto de instalação* no espaço de arquivo do AFS. O ponto de instalação é um elemento especial do sistema de arquivos que se parece e atua como um diretório comum do UNIX, mas informa ao AFS o nome do volume. ·s vezes, ao mudar para um diretório diferente (utilizando o comando **cd**, por exemplo), você *atravessa* um ponto de instalação e começa a acessar o conteúdo de um volume diferente do anterior. No entanto, geralmente você não percebe estar atravessando, pois o AFS interpreta automaticamente os pontos de instalação e recupera o conteúdo do novo diretório do volume apropriado. Não é necessário rastrear qual volume, partição ou máquina servidor de arquivos está abrigando o conteúdo de um diretório. Se, no entanto, estiver interessado, você pode saber qual é a localização de um volume; para obter instruções, consulte "Localizando Arquivos e Diretórios" na página 27.

Se o administrador do sistema seguiu o processo convencional, o seu diretório de origem corresponde a um volume, que mantém seu conteúdo agrupado em uma partição de uma máquina servidor de arquivos. Os volumes do usuário geralmente são chamados de **user.***nome do usuário*. Por exemplo, o volume para um usuário chamado **smith** na célula **abc.com** é chamado de **user.smith** e é instalado no diretório **/afs/abc.com/usr/smith**.

Como os volumes do AFS são armazenados em diferentes máquinas do servidor de arquivos, quando uma máquina torna-se indisponível apenas os volumes naquela máquina ficam inacessíveis. Os volumes armazenados em outras máquinas ainda ficam acessíveis. No entanto, quando o ponto de instalação de um volume se localiza em um volume que está armazenado em uma máquina indisponível, aquele volume também fica inacessível. Por este motivo, os volumes que contêm diretórios utilizados com freqüência (por exemplo, **/afs** e **/afs/***nome da célula*) são geralmente copiados e distribuídos para muitas máquinas do servidor de arquivos.

Quotas de Volume

Cada volume possui um limite de tamanho ou *quota*, atribuído pelo administrador do sistema. A quota de um volume determina a quantia máxima de espaço em disco que o volume pode consumir. Quando você tenta exceder a quota de um volume, você recebe uma mensagem de erro. Para obter instruções sobre a verificação da quota de volume, consulte “Exibindo a Quota de Volume” na página 25.

Os volumes possuem quotas completamente independentes. Por exemplo, suponha que o atual diretório de trabalho é **/afs/abc.com/usr/smith**, que é o ponto de instalação para o volume **user.smith** com 1000 blocos livres. Você tenta copiar um arquivo de 500 blocos do atual diretório de trabalho para o diretório **/afs/abc.com/usr/pat**, ponto de instalação para o volume **user.pat**. No entanto, você recebe uma mensagem de erro informando que não há espaço suficiente. Você verifica a quota de volume para o **user.pat** e descobre que o volume tem apenas 50 blocos livres.

Utilizando Arquivos no AFS

O Gerenciador de Cache

O espaço de arquivo do AFS pode ser acessado apenas ao se trabalhar em uma máquina cliente do AFS. O *Gerenciador de Cache* naquela máquina é o seu agente no acesso às informações armazenadas no espaço de arquivo do AFS. Quando você acessa um arquivo, o Gerenciador de Cache, em sua máquina cliente, solicita o arquivo da máquina servidor de arquivos apropriada e armazena (*coloca no cache*) uma cópia do mesmo no disco local de sua máquina cliente. Os programas de aplicação em sua máquina cliente utilizam a cópia local do arquivo colocada no cache. Isto aprimora o desempenho, pois o uso de um arquivo local é muito mais rápido do que enviar solicitações de dados do arquivo pela rede até a máquina servidor de arquivos.

Como os programas de aplicação utilizam a cópia em cache de um arquivo, todas as alterações efetuadas não são necessariamente armazenadas permanentemente na versão central armazenada na máquina servidor de arquivos até que o arquivo seja fechado. Neste ponto, o Gerenciador de Cache grava suas alterações de volta na máquina servidor de arquivos, onde elas

substituem as partes correspondentes do arquivo existente. Alguns programas de aplicação fecham um arquivo desta forma toda vez que o comando **save** é emitido (e depois reabrem o arquivo imediatamente para que você possa continuar trabalhando). Com outros programas, a emissão do comando **save** grava as alterações apenas na cópia local colocada no cache. Se você utilizar este último tipo de editor de texto, você deve fechar o arquivo periodicamente para garantir que suas alterações sejam armazenadas permanentemente.

Se uma máquina servidor de arquivos tornar-se inacessível, você pode continuar trabalhando com a cópia local do arquivo colocada no cache extraída daquela máquina, mas não pode salvar suas alterações permanentemente até que a máquina servidor fique acessível novamente.

Atualizando Cópias de Arquivos no Cache

Quando a versão central de um arquivo é alterada na máquina servidor de arquivos, o processo do *Servidor de Arquivos* do AFS sendo executado naquela máquina avisa todos os outros Gerenciadores de Cache com cópias daquele arquivo que sua versão não é mais válida. O AFS possui um mecanismo especial para realização eficiente destas notificações. Quando o Servidor de Arquivos envia ao Gerenciador de Cache uma cópia de um arquivo modificável, ele envia também um *callback*. O callback funciona como uma garantia do Servidor de Arquivos em contatar o Gerenciador de Cache se a cópia do arquivo armazenada centralmente for alterada enquanto estiver sendo utilizada. Se isto acontecer, o Servidor de Arquivos *suspende* o callback. Se você executar um programa que solicita dados do arquivo alterado, o Gerenciador de Cache observa o callback suspenso e obtém do Servidor de Arquivos uma cópia atualizada do arquivo. Os callbacks asseguram que você está trabalhando com a cópia mais recente de um arquivo.

Nota: O mecanismo de callback não garante que você veja imediatamente as alterações que outra pessoa faz em um arquivo que você esteja utilizando. O seu Gerenciador de Cache não percebe o callback suspenso até que o seu programa de aplicação solicite a ele mais dados do arquivo.

Vários Usuários Efetuando Modificações nos Arquivos

Como um sistema de arquivos padrão do UNIX, o AFS preserva apenas as alterações de um arquivo que foram salvas por último, independente de quem tiver feito as alterações. Ao colaborar com alguém nos mesmos arquivos, você deve coordenar o seu trabalho para evitar escrever por cima das alterações do outro. Você pode utilizar as listas de controle de acesso (ACLs) do AFS para limitar a capacidade de outros usuários de acessar ou alterar seus arquivos, e assim evitar que eles acidentalmente sobreponham seus arquivos. Consulte “Capítulo 4. Protegendo Seus Diretórios e Arquivos” na página 33.

Segurança do AFS

O AFS torna fácil o acesso de vários usuários aos mesmos arquivos, porém utiliza também diversos mecanismos para garantir que apenas os usuários autorizados acessem o espaço de arquivo do AFS. Os mecanismos são estes:

- As senhas e a autenticação mútua garantem que apenas os usuários autorizados acessem o espaço de arquivo do AFS
- As listas de controle de acesso permitem aos usuários restringir ou permitir o acesso aos seus próprios diretórios

Senhas e Autenticação Mútua

O AFS utiliza dois mecanismos relacionados para garantir que apenas os usuários autorizados acessem o espaço de arquivo: senhas e autenticação mútua. Os dois mecanismos requerem que o usuário comprove sua identidade.

Ao identificar-se pela primeira vez ao AFS, você deve fornecer a senha associada ao seu nome de usuário, para comprovar que é quem está dizendo ser. Ao fornecer a senha correta, você é *autenticado* e o seu Gerenciador de Cache recebe um *token*. O token é um pacote de informações embaralhadas por um programa de autenticação do AFS que utiliza sua senha do AFS como uma chave. O seu Gerenciador de Cache pode desembaralhar o token porque ele conhece sua senha e o método de embaralhamento do AFS.

O token age como prova aos programas de servidor do AFS que você está autenticado como um usuário válido do AFS. Ele serve como a base para o segundo meio pelo qual o AFS cria a segurança, chamado de *autenticação mútua*. Na autenticação mútua, as duas partes comunicando-se pela rede comprovam suas identidades entre si. O AFS requer a autenticação mútua sempre que um servidor e o cliente (geralmente, um Gerenciador de Cache) comunicam-se entre si.

O protocolo de autenticação mútua que o AFS utiliza foi projetado para tornar muito difícil autenticações fraudulentas. Quando o seu Gerenciador de Cache contata um Servidor de Arquivos em seu nome, ele envia o token obtido em sua autenticação. O token é codificado com uma chave que somente um Servidor de Arquivos do AFS pode saber. Se o Servidor de Arquivos puder descodificar o seu token, ele pode comunicar-se com o seu Gerenciador de Cache. Sucessivamente, o Gerenciador de Cache aceita o Servidor de Arquivos como autêntico porque o Servidor de Arquivos pode descodificar e utilizar as informações no token.

Listas de Controle de Acesso

O AFS utiliza as *listas de controle de acesso* (*ACLs*) para determinar quem pode acessar as informações no espaço de arquivo do AFS. Cada diretório do AFS possui um ACL para especificar que ações os diferentes usuários podem

executar naquele diretório e seus arquivos. Um ACL pode conter aproximadamente 20 entradas para os usuários, os grupos, ou ambos; cada entrada lista um usuário ou grupo e as permissões que ele possui.

O proprietário de um diretório e os administradores do sistema sempre podem administrar um ACL. Os diretórios de origem e subdiretórios pertencem automaticamente aos usuários. Outros usuários que não sejam proprietários podem definir o ACL de um diretório somente se esta permissão lhe for especificamente concedida no ACL. Para obter mais informações sobre os ACLs, consulte "Capítulo 4. Protegendo Seus Diretórios e Arquivos" na página 33 .

Um grupo é composto por um ou mais usuários e máquinas do cliente. Se um usuário pertence a um grupo que aparece em um ACL, o usuário obtém todas as permissões concedidas a aquele grupo, exatamente como se o usuário tivesse sido listado diretamente no ACL. De modo semelhante, se um usuário estiver conectado a uma máquina cliente que pertence a um grupo, o usuário possui todas as permissões concedidas a aquele grupo. Para obter instruções sobre a definição e uso de grupos, consulte "Capítulo 5. Utilizando Grupos" na página 51.

Todos os usuários que podem acessar o espaço de arquivo de sua célula, autenticados ou não, são automaticamente atribuídos a um grupo chamado de **system:anyuser**. Para obter uma explicação sobre a colocação do grupo **system:anyuser** nas ACLs, consulte "Estendendo o Acesso aos Usuários de Células Externas" na página 38.

Nota: Você pode usar os bits de modo do UNIX para controlar o acesso em arquivos específicos dentro de um diretório do AFS; no entanto, o efeito destes bits de modo é diferente no AFS e no sistema de arquivos padrão do UNIX. Consulte "Proteção de Arquivo e de Diretório" na página 8.

Diferenças Entre o UNIX e o AFS

O AFS foi projetado para ser semelhante ao sistema de arquivos UNIX. Por exemplo, vários dos comandos básicos de manipulação de arquivos do UNIX (**cp** para cópia, **rm** para remoção e assim por diante) são iguais no AFS e no UNIX. Todos os seus programas de aplicação funcionam como antes. As seções a seguir descrevem algumas das diferenças entre um sistema de arquivos padrão UNIX e AFS.

Compartilhamento de Arquivos

O AFS permite aos usuários compartilhar arquivos remotos com a mesma facilidade dos arquivos locais. Para acessar um arquivo em uma máquina remota no AFS, você simplesmente especifica o nome do caminho do arquivo.

Em comparação, para acessar um arquivo no sistema de arquivos UNIX de uma máquina remota, você deve conectar-se à máquina remota ou criar um ponto de instalação na máquina local que indique um diretório no sistema de arquivos UNIX da máquina remota.

Os usuários do AFS podem ver e compartilhar todos os arquivos sob o diretório raiz **/afs**, concedidos os privilégios adequados. Um usuário do AFS que possui os privilégios necessários pode acessar um arquivo em qualquer célula do AFS, simplesmente especificando o nome de caminho do arquivo. O compartilhamento de arquivos no AFS não é limitado por distâncias geográficas ou diferenças do sistema operacional.

Login e Autenticação

Para tornar-se um usuário do AFS autenticado, você deve fornecer uma senha ao AFS.

- Em máquinas que utilizam um utilitário de login modificado pelo AFS, o login é um processo de uma única etapa; o seu login inicial efetua sua autenticação automaticamente com o AFS.
- Em máquinas que não utilizam um utilitário de login modificado pelo AFS, é necessária a realização de duas etapas.
  1. Efetue o login em sua máquina local.
  2. Emita o comando **klog** com o argumento **-setpag** para fazer a autenticação com o AFS e receber seu token.

O administrador do sistema pode informar se sua máquina utiliza ou não um utilitário de login modificado pelo AFS. Depois, consulte as instruções de login em “Efetuando o Login e a Autenticação com o AFS” na página 13.

As senhas de autenticação do AFS são armazenadas em um banco de dados especial do AFS, e não no arquivo de senhas local (**/etc/passwd** ou equivalente). Se a sua máquina utiliza um utilitário de login modificado pelo AFS, você pode alterar sua senha com um único comando. Se a sua máquina não utiliza este utilitário, você deve emitir comandos separados para alterar suas senhas do AFS e local. Consulte “Alterando Sua Senha” na página 21.

Proteção de Arquivo e de Diretório

O AFS não se apoia nas proteções de bit de modo de um sistema UNIX padrão (embora seu sistema de proteção interaja com estes bits de modo). Ao invés disso, o AFS utiliza uma lista de controle de acesso (ACL) para controlar o acesso a cada diretório e seu conteúdo. A lista abaixo sintetiza as diferenças entre os dois métodos:

- Os bits de modo do UNIX especificam três tipos de permissões de acesso: **r** (**ler**), **w** (**gravar**) e **x** (**executar**). Um ACL do AFS utiliza sete tipos de permissões: **r** (**ler**), **l** (**procurar**), **i** (**inserir**), **d** (**excluir**), **w** (**gravar**), **k**

(**bloquear**) e **a** (**administrar**). Para obter mais informações, consulte “As Permissões ACL AFS” na página 34 e “Como o AFS Usa os Bits de Modo UNIX” na página 48.

- Os três conjuntos de bits de modo em cada arquivo ou diretório do UNIX permitem a você conceder permissões a três usuários ou grupos de usuários: o proprietário do arquivo ou diretório, o grupo que possui o arquivo ou diretório e todos os outros usuários. Um ACL pode acomodar até aproximadamente 20 entradas, cada uma das quais estende certas permissões a um usuário ou grupo. Ao contrário do UNIX padrão, um usuário pode pertencer a um número ilimitado de grupos, e os grupos podem ser definidos pelos usuários e pelos administradores do sistema. Consulte “Capítulo 5. Utilizando Grupos” na página 51.
- Os bits de modo do UNIX são definidos individualmente em cada arquivo e diretório. Um ACL aplica-se a todos os arquivos em um diretório. Enquanto que, à primeira vista, o método do AFS possivelmente parece ser menos preciso, na realidade (dada uma estrutura de diretórios adequada) não há grandes desvantagens em relação às proteções de nível de diretório e elas são mais fáceis de serem estabelecidas e mantidas.

Períodos de Inatividade das Máquinas

Os tipos de falhas pelos quais você passa quando um sistema de arquivos padrão do UNIX fica inativo são diferentes de quando uma ou mais máquinas individuais do servidor de arquivos do AFS ficam indisponíveis. Quando um sistema de arquivos padrão do UNIX fica inacessível, o sistema simplesmente fica bloqueado e você pode perder as alterações efetuadas nos arquivos em que você estava trabalhando.

Quando uma máquina servidor de arquivos do AFS fica inacessível, os arquivos daquela máquina não podem ser acessados. No entanto, se uma cópia do arquivo estiver disponível a partir de outra máquina servidor de arquivos, você não percebe necessariamente a inatividade do servidor. Isto porque o AFS concede aos administradores do sistema da sua célula a capacidade de armazenar cópias de programas comuns em vários servidores de arquivos. O Gerenciador de Cache opta automaticamente entre as cópias; quando uma cópia torna-se indisponível, o Gerenciador de Cache simplesmente escolhe outra.

Se não houver outras cópias de um arquivo que esteja armazenado em uma máquinas do servidor inacessível, você geralmente pode continuar a usar a cópia armazenada no cache local do AFS de sua máquina cliente. No entanto, não é possível salvar alterações em arquivos armazenados em uma máquina servidor de arquivos inacessível até que ela torne-se acessível novamente.

Comandos Remotos

Os *comandos remotos* do UNIX permitem ao usuário executar programas em uma máquina remota sem estabelecer uma conexão com ela utilizando um

programa como o **telnet**. Muitos dos comandos remotos (como **ftp**, **rcp** e **rsh**) continuam disponíveis no AFS, dependendo de como seus administradores configuraram os mesmos. Se a máquina remota possuir um Gerenciador de Cache, seu token também é utilizado lá e você é autenticado à medida que o comando remoto é executado. Se a máquina remota não executa um Gerenciador de Cache, você recebe a seguinte mensagem:

```
Aviso: não é possível fazer a autenticação.
```

Neste caso, você está conectado ao sistema de arquivos UNIX da máquina remota, mas não está autenticado no AFS. Você pode acessar os arquivos locais na máquina remota e os diretórios do AFS que concedem acesso ao grupo **system:anyuser**, mas não pode acessar diretórios protegidos do AFS.

Diferenças na Semântica dos Comandos Padrão do UNIX

Esta seção sintetiza as diferenças na funcionalidade de alguns comandos do UNIX regularmente emitidos.

chmod
: Somente os membros do grupo **system:administrators** podem usar este comando para ativar a setuid, setgid ou os bits de modo sticky em arquivos do AFS. (Para obter maiores informações sobre este grupo, consulte "Utilizando os Grupos do Sistema em ACLs" na página 37.)

chown
: Somente os membros do grupo **system:administrators** podem emitir este comando em arquivos do AFS.

chgrp
: Somente membros do grupo **system:administrators** podem emitir este comando em arquivos e diretórios do AFS.

groups
: Se os tokens AFS do usuário estiverem identificados por um grupo de autenticação do processo (PAG), a saída deste comando inclui dois números grandes. Para ver uma descrição dos PAGs, consulte "Efetuando a Autenticação com o AFS" na página 14.

inetd
: A versão do AFS deste daemon autentica os emissores remotos dos comandos **rcp** e **rsh** modificados pelo AFS com o AFS.

login utilities
: Os utilitários de login modificados pelo AFS efetuam o seu login no sistema de arquivos local do UNIX e efetuam sua autenticação no AFS.

ln
: Este comando não pode ser usado para criar uma ligação de hardware entre os arquivos que se localizam em diretórios diferentes do AFS. É preciso incluir a opção **-s** para criar em seu lugar uma ligação simbólica.

Utilizando o AFS com o NFS

Algumas células utilizam o Networking File System (NFS) em acréscimo ao AFS. Se você trabalha em uma máquina cliente do NFS, o administrador do sistema pode configurá-la para acessar o espaço de arquivo do AFS através de um programa chamado *NFS/AFS Translator*™. Consulte "Apêndice A. Utilizando o NFS/AFS Translator" na página 73.

Capítulo 2. Utilizando o AFS

Este capítulo explica como executar quatro tarefas básicas do AFS: efetuar o login e a autenticação, encerrar uma sessão, acessar o espaço de arquivo e alterar sua senha.

Efetuando o Login e a Autenticação com o AFS

Para acessar o espaço de arquivo do AFS como um usuário autenticado, você precisa efetuar o login em um sistema de arquivos (UNIX) local da máquina cliente do AFS e fazer a autenticação com o AFS. Ao efetuar o login, você estabelece sua identidade do sistema local. Ao efetuar a autenticação, você comprova sua identidade ao AFS e obtém um token, o qual o seu Gerenciador de Cache utiliza para comprovar seu status autenticado aos processos do servidor do AFS que ele contata em seu nome. Os usuários que não são autenticados (que não possuem um token) possuem acesso limitado aos diretórios e arquivos do AFS.

Efetuando o Login

Em máquinas que utilizam um utilitário de login modificado pelo AFS, o login e a autenticação são feitos em uma etapa. Em máquinas que não utilizam um utilitário de login modificado pelo AFS, você efetua o login e a autenticação em etapas separadas. Para determinar o tipo de utilitário de login que sua máquina utiliza, você pode verificar os tokens do AFS depois de efetuar o login ou perguntar ao administrador do sistema, que também pode lhe informar sobre qualquer diferença entre o seu procedimento de login e os dois métodos aqui descritos.

Efetuando o Login Utilizando um Utilitário de Login modificado pelo AFS

Forneça seu nome de usuário no prompt `login:` que aparece quando você estabelece uma nova conexão com uma máquina. Depois, forneça sua senha no prompt `Senha:` como mostrado no seguinte exemplo. (Sua senha não é reproduzida visivelmente na tela.)

```
login: nome do usuário
Senha: senha
```

Se não estiver certo em relação ao tipo de utilitário de login sendo executado em sua máquina, é melhor emitir o comando **tokens** para verificar se você está autenticado; para obter instruções, consulte “Exibindo Seus Tokens” na página 17. Caso não possua tokens, emita o comando **klog**, descrito em “Efetuando a Autenticação com o AFS” na página 16.

Efetuando o Login Utilizando um Procedimento de Duas Etapas

Se a sua máquina não utiliza um utilitário de login modificado pelo AFS, você deve executar um procedimento de duas etapas:

1. Efetue o login no sistema de arquivos local da sua máquina cliente fornecendo um nome de usuário e senha nos prompts **login** do programa.
2. Emita o comando **klog** para fazer a autenticação com o AFS. Acrescente o argumento **-setpag** do comando para associar seu token a um número de identificação especial chamado *PAG* (para *process authentication group*). Para ver uma descrição dos PAGs, consulte "Protegendo Seus Tokens com um PAG".

```
% klog -setpag
Senha: sua_senha_AFS
```

Nota: Se a sua máquina utiliza um procedimento de login de duas etapas, você pode optar pelo uso de senhas diferentes para efetuar o login e a autenticação. Embora seja mais simples utilizar a mesma senha para ambos. Consulte o administrador do sistema.

Efetuando a Autenticação com o AFS

Para trabalhar com maior eficiência no espaço de arquivo do AFS, você deve efetuar a autenticação com o AFS. Ao fazê-la, o Gerenciador de Cache recebe um token como prova de seu status de autenticado. Ele utiliza o token ao solicitar serviços dos servidores do AFS, que aceitam o token como prova de seu status de autenticado. Caso não possua um token, os servidores do AFS o consideram como sendo o usuário **anônimo** e seu acesso ao espaço de arquivo do AFS é limitado: você tem apenas as permissões do ACL concedidas ao grupo **system:anyuser**.

Você pode obter novos tokens (reautenticar) a qualquer momento, mesmo depois de usar um utilitário de login modificado pelo AFS, que efetua seu login e sua autenticação em uma etapa. Emita o comando **klog** descrito em "Efetuando a Autenticação com o AFS" na página 16.

Protegendo Seus Tokens com um PAG

Para tornar seu acesso ao AFS o mais seguro possível, é melhor associar seus tokens a um número de identificação exclusivo chamado *PAG* (para *process authentication group*). Os utilitários de login modificados pelo AFS criam automaticamente um PAG e associam o novo token a ele. Para criar um PAG ao utilizar o procedimento de login de duas etapas, inclua o sinalizador **-setpag** do comando **klog**. Se este sinalizador não for utilizado, seus tokens são associados a um número de UID do UNIX. Este tipo de associação possui dois possíveis drawbacks:

- Qualquer pessoa que assume sua identidade local do UNIX pode utilizar seus tokens. A **raiz** do superusuário local pode utilizar sempre o comando **su** do UNIX para assumir sua UID do UNIX, mesmo sem saber sua senha.

- Em alguns ambientes, determinados programas não podem utilizar seus tokens mesmo em ocasiões apropriadas para fazê-lo. Por exemplo, os comandos de impressão como **lp** ou **lpr** possivelmente não podem acessar os arquivos que você deseja imprimir, pois não podem utilizar seus tokens.

Obtendo Tokens Para Células Externas

Um token é válido apenas em uma célula (a célula cujo serviço de autenticação do AFS o emitiu). Os processos do servidor do AFS em qualquer outra célula o consideram como sendo o usuário **anônimo** a menos que você tenha uma conta na célula e tenha efetuado a autenticação com seu serviço de autenticação do AFS.

Para obter tokens em uma célula externa, utilize o argumento **-cell** para o comando **klog**. Você pode ter tokens para sua célula pessoal e uma ou mais células externas ao mesmo tempo.

A Regra Um-Token-Por-Célula

Você pode ter apenas um token por célula para cada PAG obtido em uma máquina cliente. Caso já tenha um token para uma determinada célula e emita o comando **klog**, o novo token substitui o existente. A obtenção de um novo token é útil quando seu token atual está quase expirado e você deseja continuar acessando os arquivos do AFS. Para ver uma explicação sobre a expiração de tokens, consulte "Duração do Token".

Para obter um segundo token para a mesma célula, você deve efetuar o login em uma máquina diferente ou estabelecer outra conexão separada com a máquina na qual já possui um token (utilizando o utilitário **telnet**, por exemplo). Você recebe um novo PAG para cada máquina ou conexão separada e pode usar os tokens associados apenas enquanto estiver trabalhando naquela máquina ou conexão.

Obtendo Tokens como Outro Usuário

Você pode efetuar a autenticação com outro nome de usuário se souber a senha associada. (É claro que não é ético utilizar os tokens de outro usuário sem permissão.) Se você utilizar o comando **klog** para efetuar a autenticação como outro nome de usuário do AFS, você retém sua própria identidade local (UNIX), mas os processos do servidor do AFS o reconhecem como o outro usuário. O novo token substitui qualquer token que você já tenha para a célula relevante (pelo motivo descrito em "A Regra Um-Token-Por-Célula").

Duração do Token

Os tokens possuem duração limitada. Para determinar quando expiram os seus tokens, emita o comando **tokens**, como descrito em "Exibindo Seus Tokens" na página 17. Se em alguma ocasião não conseguir acessar o AFS da forma como normalmente faz, a emissão do comando **tokens** informa se um token expirado seria o possível motivo.

Os administradores da célula definem a duração padrão do seu token. O serviço de autenticação do AFS nunca concede a um token um período de duração superior ao padrão, mas você pode solicitar um período inferior. Consulte a página de referência do **klog** no *AFS Administration Reference* para saber como usar o argumento **-lifetime** para este fim.

Efetuando a Autenticação para o Acesso ao DFS

Se a sua máquina estiver configurada para acessar o espaço de arquivo do DFS da célula do DCE através do AFS/DFS Migration Toolkit, você pode utilizar o comando **dlog** para efetuar a autenticação com o DCE. O comando **dlog** não possui efeito algum em sua capacidade de acesso ao espaço de arquivo do AFS.

Se o administrador do sistema tiver convertido sua conta do AFS em conta do DCE e você não está certo de sua senha do DCE, utilize o comando **dpass** para exibi-la. Você deve estar autenticado como o usuário do AFS cuja conta do AFS foi convertida em conta do DCE e deve poder fornecer a senha correta do AFS. Assim como o comando **dlog**, o comando **dpass** não tem qualquer funcionalidade em relação ao AFS.

Para obter maiores informações sobre o uso dos comandos **dlog** e **dpass**, consulte o administrador do sistema.

Efetuando a Autenticação com o AFS

Se a sua máquina não estiver usando um utilitário de login modificado pelo AFS, você deve efetuar a autenticação após o login emitindo o comando **klog**. Este comando também pode ser emitido a qualquer hora para obtenção de um token com uma data de expiração posterior a do seu token atual.

```
% klog [-setpag] [-cell <cell name>]
Senha: sua_senha_AFS
```

em que

-setpag
: Associa os tokens resultantes a um PAG (consulte “Protegendo Seus Tokens com um PAG” na página 14). Acrescente este sinalizador na primeira vez que obtém um token para uma célula específica durante uma sessão de login ou conexão. Não o acrescente quando estiver atualizando o token para uma célula durante a mesma sessão.

-cell
: Atribui nome à célula para a qual irá obter o token. É necessário ter uma conta na célula.

Sua senha não é reproduzida visivelmente na tela. Quando o prompt do shell retorna, você é um usuário autenticado do AFS. Você pode usar o comando **tokens** para verificar se está autenticado, como descrito na seção seguinte.

Exibindo Seus Tokens

Utilize o comando **tokens** para exibir seus tokens.

```
% tokens
```

A seguinte saída indica que você não possui tokens:

```
Tokens mantidos pelo Gerenciador de Cache:
    --Fim da lista--
```

Se você tiver um ou mais tokens, a saída se parece com o exemplo a seguir, no qual os tokens para UID do AFS 1022 na célula **abc.com** expiram em 3 de Agosto às 14:35. Os tokens para a UID do AFS 9554 na célula **stateu.edu** expiram em 4 de Agosto à 0:02.

```
Tokens mantidos pelo Gerenciador de Cache:
Tokens do usuário (ID do AFS 1022) para afs@abc.com [Expiram Ag 3 14:35]
Tokens do usuário (ID do AFS 9554) para afs@stateu.edu [Expiram Ag 4 1:02]
    --Fim da lista--
```

Exemplo: Efetuando Autenticação na Célula Local

Suponha que o usuário **terry** não pode salvar um arquivo. Ele utiliza o comando **tokens** e descobre que seus tokens expiraram. Ele efetua a reautenticação em sua célula local sob sua atual identidade emitindo o seguinte comando:

```
% klog
Senha:  senha_de_terry
```

Depois, ele emite o comando **tokens** para certificar-se de que está autenticado.

```
% tokens
Tokens mantidos pelo Gerenciador de Cache:
Tokens do usuário (ID do AFS 4562) para afs@abc.com [Expiram Jun 22 14:35]
    --Fim da lista--
```

Exemplo: Efetuando a Autenticação como Outro Usuário

Agora, o **terry** efetua a autenticação em sua célula local como outro usuário, **pat**. O novo token substitui o token existente do **terry**, pois o Gerenciador de Cache pode armazenar apenas um token por célula por sessão de login em uma máquina.

```
% klog pat
Senha: senha_de_pat
% tokens
Tokens mantidos pelo Gerenciador de Cache:
Tokens do usuário (ID do AFS 4278) para afs@abc.com [Expiram Jun 23 9:46]
    --Fim da lista--
```

Exemplo: Efetuando a Autenticação em uma Célula Externa

Agora, o **terry** efetua a autenticação na célula **stateu.edu** em que sua conta é chamada de **ts09**.

```
% klog  ts09 -cell stateu.edu
Senha: senha_de_ts09
% tokens
Tokens mantidos pelo Gerenciador de Cache:
Tokens do usuário (ID do AFS 4562) para afs@abc.com [Expiram Jun 22 14:35]
Tokens do usuário (ID do AFS 8346) para afs@stateu.edu [Expiram Jun 23 1:02]
    --Fim da lista--
```

Limites em Tentativas Falhas de Autenticação

O administrador do sistema pode optar por limitar o número de vezes que você falha em fornecer a senha correta ao efetuar a autenticação com o AFS (utilizando um utilitário de login modificado pelo AFS ou o comando **klog**). Se o limite for excedido, o serviço de autenticação do AFS recusa outras tentativas de autenticação por um período de tempo definido pelo administrador do sistema. A finalidade deste limite é impedir que usuários não autorizados invadam a sua conta tentando com uma série de senhas.

Para determinar se a sua conta de usuário está sujeita a este limite, pergunte ao administrador do sistema ou emita o comando **kas examine**, como descrito em "Exibindo o Limite de Autenticação Falha e o Tempo de Bloqueio".

A mensagem a seguir indica que você excedeu o limite de tentativas de autenticação falhas.

```
Não foi possível fazer a autenticação para o AFS porque a ID
está bloqueada - consulte o admin do sistema
```

Exibindo o Limite de Autenticação Falha e o Tempo de Bloqueio

Emita o comando **kas examine** para determinar se há um limite no número de tentativas de autenticação sem êxito para sua conta de usuário e algum tempo de lockout associado. Você pode examinar apenas sua própria conta. A quarta linha da saída reporta o número máximo de vezes que você pode fornecer uma senha incorreta antes de ficar com sua conta bloqueada. O campo `tempo de bloqueio` na linha seguinte reporta por quanto tempo o serviço de autenticação do AFS recusa tentativas de autenticação depois que o limite é excedido.

```
% kas examine seu_nome_de_usuário
Senha para seu_nome_de_usuário: sua_senha_AFS
```

O exemplo a seguir exibe a saída para o usuário **pat**, que pode ter nove tentativas de autenticações falhas. O tempo de bloqueio é de 25.5 minutos.

```
Dados de usuário para o pat
 key (15) cksum é 3414844392,  último cpw: 21 Out Qui 16:05:44 1999
 senha expira em:  Sex 26 Nov 20:44:36 1999
 9 autenticações consecutivas sem êxito são permitidas.
 O tempo de bloqueio para este usuário é de 25.5 minutos.
 O usuário não está bloqueado.
 entrada nunca expira. Duração máx. do ticket 100.00 horas.
 última mod em 18 Ago Qua 08:22:29 1999 feita pelo admin
 permite reutilização da senha
```

Saindo de uma Sessão do AFS

Como o login e a autenticação com o AFS são operações distintas, é preciso efetuar o logout e a eliminação de autenticação (emita o comando **unlog** para descartar seus tokens) ao sair de uma sessão do AFS. A simples efetuação do logout não remove necessariamente os seus tokens.

Você pode usar o comando **unlog** quando desejar para fazer a eliminação de autenticação, não apenas quando estiver efetuando o logout. Por exemplo, é uma boa prática efetuar a eliminação de autenticação antes de deixar uma máquina não-assistida, para impedir que outros usuários utilizem seus tokens durante sua ausência. Ao retornar à máquina, emita o comando **klog** para efetuar a reautenticação, como descrito em "Efetuando a Autenticação com o AFS" na página 16.

Não emita o comando **unlog** quando estiver executando trabalhos que levam muito tempo para serem concluídos, mesmo que esteja efetuando o logout. Tais processos precisam ter um token durante o tempo todo que precisarem de acesso autenticado ao AFS.

Se tiver tokens de várias células e deseja descartar apenas alguns deles, acrescente o argumento **-cell** do comando **unlog**.

Destacando Tokens

Emita o comando **unlog** para descartar seus tokens:

```
% unlog -cell  <name da célula>+
```

Omita o argumento **-cell** para descartar todos os seus tokens, ou utilize-o para indicar cada célula para a qual irá descartar os tokens. Seria melhor fornecer o nome completo de cada célula (como **stateu.edu** ou **abc.com**).

Você pode emitir o comando **tokens** para verificar se seus tokens foram destruídos, como no seguinte exemplo.

```
% tokens
Tokens mantidos pelo Gerenciador de Cache:
    --Fim da lista--
```

Exemplo: Elimando a autenticação a partir de uma Célula Específica

No exemplo a seguir, um usuário possui tokens nas células **accounting** e **marketing** de sua empresa. Ele descarta o token para a célula **acctg.abc.com** mas mantém o token para a célula **mktg.abc.com**.

```
% tokens
Tokens mantidos pelo Gerenciador de Cache:
Tokens do usuário (ID do AFS 35) para afs@acctg.abc.com
[Expiram Nov 10 22:30]
Tokens do usuário (ID do AFS 674) para afs@mktg.abc.com
[Expiram Nov 10 18:44]
    --Fim da lista--
```

```
% unlog -cell acctg.abc.com
% tokens
Tokens mantidos pelo Gerenciador de Cache:
Tokens do usuário (ID do AFS 674) para afs@mktg.abc.com
[Expiram Nov 10 18:44]
    --Fim da lista--
```

Efetuando o Logout

Depois de eliminar a autenticação, efetue o logout emitindo o comando apropriado ao seu tipo de máquina, possivelmente um dos seguintes.

```
% logout
```

ou

```
% exit
```

ou

```
% <Ctrl-d>
```

Acessando o Espaço de Arquivo do AFS

Enquanto você está conectado (login) e autenticado, você pode acessar arquivos no AFS exatamente como fez no sistema de arquivos UNIX. A única diferença é que você pode acessar muito mais arquivos. Assim como no sistema de arquivos UNIX, você pode acessar apenas aqueles arquivos para os quais tem permissão. O AFS utiliza as listas de controle de acesso (ACLs) para controlar o acesso, como descrito em “Capítulo 4. Protegendo Seus Diretórios e Arquivos” na página 33.

Nomes de Caminho do AFS

Os nomes de caminho do AFS são muito parecidos com os nomes de sistema de arquivos do UNIX. A principal diferença é que todos os nomes de caminho do AFS começam com o diretório raiz do AFS, que é chamado, por convenção, de **/afs**. Ter o **/afs** no topo de cada espaço de arquivo da célula do AFS agrupa os espaços de arquivo em um espaço de arquivo global.

Nota aos usuários do Windows: O Windows utiliza uma barra invertida (****) ao invés de uma barra normal (**/**) para separar os elementos em um nome de caminho. Quanto ao resto, seu acesso ao espaço de arquivo do AFS é praticamente igual ao de usuários trabalhando em máquinas UNIX.

O segundo elemento nos nomes de caminho do AFS geralmente é o nome de uma célula. Por exemplo, a célula da Corporação ABC é chamada de **abc.com** e e o nome de caminho de todos os arquivos em seu espaço de arquivo começam com a cadeia **/afs/abc.com**. Algumas células também criam um diretório no segundo nível com um nome mais curto (tal como **abc** para **abc.com** ou **stateu** para **stateu.edu**), para reduzir a digitação necessária. O administrador do sistema pode lhe informar se o espaço de arquivo de sua

célula contém nomes mais curtos como este. O resto do nome do caminho depende de como o administrador da célula organizou seu espaço de arquivo.

Para acessar diretórios e arquivos no AFS, você deve especificar o nome de caminho completo e deve possuir as permissões necessárias no ACL que protegem o diretório e os arquivos nele contidos.

Exemplo: Exibindo o Conteúdo do Diretório de Outro Usuário

O usuário **terry** que procurar por um arquivo que pertence a outro usuário, **pat**. Ele emite o comando **ls** no nome de caminho apropriado.

```
% ls /afs/abc.com/usr/pat/public
doc/                    directions/
guide/                  jokes/
library/
```

Acessando Células Externas

Você pode acessar arquivos não apenas em sua própria célula, mas em qualquer célula do AFS que você possa alcançar pela rede, independente da localização geográfica. Há dois requisitos adicionais:

- A lista de células externas do seu Gerenciador de Cache deve conter a célula que você deseja acessar. Apenas o **raiz** do superusuário local pode editar a lista de células, mas qualquer pessoa pode exibi-la. Consulte “Determinando o Acesso a Células Externas” na página 29.
- O ACL, no diretório que abriga o arquivo e em todos os diretórios pai no nome de caminho, deve conceder a você as permissões necessárias. A forma mais simples do proprietário do diretório estender permissões a usuários estrangeiros é colocando uma entrada para o grupo **system:anyuser** no ACL.

  A alternativa seria o administrador da célula externa criar uma conta para você, transformando você essencialmente em um usuário local da célula. O proprietário do diretório cria uma entrada do ACL para você como para qualquer outro usuário local. Para fazer a autenticação na célula externa, emita o comando **klog** com o argumento **-cell**.

Para outras explicações sobre a proteção de diretórios e arquivos, consulte “Capítulo 4. Protegendo Seus Diretórios e Arquivos” na página 33.

Alterando Sua Senha

Nas células que utilizam o utilitário de login modificado pelo AFS, a senha é a mesma para o login e autenticação com o AFS. Neste caso, você utiliza um único comando, **kpasswd**, para alterar a senha.

Se a sua máquina não utiliza um utilitário de login modificado pelo AFS, há senhas separadas para o login no sistema de arquivos local e a autenticação com o AFS. (As duas senhas podem ser iguais ou diferentes, à sua escolha.)

Neste caso, utilize o comando **kpasswd** para alterar sua senha do AFS e o comando **passwd** do UNIX para alterar sua senha do UNIX.

O administrador do sistema pode melhorar a segurança da célula configurando diversos recursos que orientam sua escolha da senha. Considere-os ao emitir o comando **kpasswd**:

- Limitar o período de tempo que sua senha é válida. Isto melhora a segurança de sua célula limitando o período de tempo que um usuário não-autorizado tem para tentar adivinhar sua senha. O administrador do sistema precisa lhe informar quando sua senha irá expirar para que você possa alterá-la a tempo. O administrador pode configurar o utilitário de login modificado pelo AFS para reportar estas informações automaticamente toda vez que você efetua o login. Você também pode usar o comando **kas examine** para exibir a data de expiração da senha, como explicado em "Exibindo a Data de Expiração e os Critérios de Reutilização das Senhas".

  Você pode alterar sua senha antes da data de expiração, mas o administrador do sistema pode optar por definir um período mínimo entre as trocas de senhas. A mensagem a seguir indica que o período mínimo ainda não passou.

  ```
  kpasswd:  a senha não foi alterada porque havia sido alterada muito
  recentemente; consulte o administrador do sistema
  ```
- Impor padrões de qualidade de senha, como tamanho mínimo ou a inclusão de caracteres não-alfabéticos. O administrador precisa lhe informar sobre tais requisitos para que você não perca tempo escolhendo senhas inaceitáveis.
- Rejeitar uma senha que é muito parecida com as 20 últimas senhas que você utilizou. Você pode usar o comando **kas examine** para verificar se este critério aplica-se a você, como explicado em "Exibindo a Data de Expiração e os Critérios de Reutilização das Senhas". A mensagem a seguir indica que a senha escolhida é muito parecida com a anterior.

  ```
  kpasswd:  A senha não foi alterada porque parece ser uma senha reutilizada
  ```

Exibindo a Data de Expiração e os Critérios de Reutilização das Senhas

Emita o comando **kas examine** para exibir a data de expiração e os critérios de reutilização da senha. Você pode examinar apenas sua própria conta. A terceira linha da saída constata a data de expiração da senha. A última linha indica os critérios de reutilização da senha que se aplicam a você.

```
% kas examine seu_nome_de_usuário
Senha para seu_nome_de_usuário: sua_senha_AFS
```

O exemplo a seguir exibe a saída para o usuário **pat**.

```
Dados de usuário para o pat
 key (15) cksum é 3414844392,  último cpw: 21 Out Qui 16:05:44 1999
 senha expira em:  Sex 26 Nov 20:44:36 1999
```

```
9 autenticações consecutivas sem êxito são permitidas.
O tempo de bloqueio para este usuário é de 25.5 minutos.
O usuário não está bloqueado.
entrada nunca expira. Duração máx. do ticket 100.00 horas.
última mod em 18 Ago Qua 08:22:29 1999 feita pelo admin
não permite reutilização da senha
```

Alterando Sua Senha do AFS

Emita o comando **kpasswd**, que pede que você forneça suas senhas antiga e nova e que confirme a senha nova. As senhas não são reproduzidas visivelmente na tela.

```
% kpasswd
Senha antiga: senha_atual
Senha nova (RETURN para interromper): senha_nova
Re-digite a senha nova: senha_nova
```

Alterando Sua Senha do UNIX

Emita o comando **passwd** do UNIX, que pede que você forneça suas senhas antiga e nova e que confirme a senha nova. As senhas não são reproduzidas visivelmente na tela. Em várias máquinas, a **passwd** se localiza no diretório **/bin** e é possível que você precise digitar o nome de caminho completo.

```
% passwd
Alterando a senha para nome_de_usuário.
Senha antiga: senha_atual
Senha nova: senha_nova
Re-digite a senha nova: senha_nova
```

Capítulo 3. Exibindo as Informações sobre o AFS

Este capítulo explica como exibir informações que podem ajudar você a usar o AFS mais efetivamente. Ele inclui as seguintes seções.

Exibindo a Quota de Volume

Por convenção, os arquivos do diretório de origem são armazenados juntos em um único volume. (Para obter informações sobre volumes, consulte “Volumes e Pontos de Instalação” na página 3.) Para alocar o espaço em disco disponível da célula da melhor maneira possível, os administradores do sistema impõem um limite de tamanho ou uma *quota* a cada volume. Você não pode armazenar mais dados em um volume do que sua quota permite. Se um volume estiver perto de sua quota, você talvez não consiga salvar as alterações feitas em arquivos armazenados no volume.

A quantidade de espaço disponível na partição que abriga o volume também limita o crescimento do volume. Se a partição de disco estiver cheia, é possível que você não consiga salvar alterações de um arquivo mesmo que o volume não esteja próximo de sua quota.

Verifique a quota do seu volume pessoal periodicamente para ter certeza de que tem espaço adequado. Se encontrar problemas ao salvar um arquivo, confira a quota de volume em que o arquivo foi armazenado. Use os seguintes comandos para exibir a quota de volume.

- O comando **fs quota** lista a porcentagem da quota de volume utilizada.
- Ambos os comandos **fs listquota** e **fs examine** listam o nome do volume, seu tamanho máximo (quota) e seu tamanho atual. Eles também relatam as seguintes informações adicionais.
  - O comando **fs listquota** lista a porcentagem usada tanto do volume, quanto da partição.
  - O comando **fs examine** lista o tamanho da partição, a quantidade de espaço usado atualmente e todas as mensagens associadas ao volume.

Exibindo a Porcentagem da Quota Usada

Emita o comando **fs quota** para exibir a porcentagem da quota utilizada atualmente do volume que contém um diretório ou arquivo especificado.

```
% fs quota [<caminho do direório/arquivo>+]
```

sendo que *caminho do diretório/arquivo* especifica o nome de caminho de um arquivo ou diretório em cada volume do qual serão exibidas informações da quota. Se você não fornecer um nome de caminho, a saída relatará as informações da quota de volume que contém o diretório do trabalho atual.

Exemplo: Exibindo a Porcentagem da Quota Usada

O exemplo a seguir mostra a porcentagem da quota usada nos volumes que contêm dois diretórios de origem de usuário na célula ABC Corporation.

```
% cd /afs/abc.com/usr
% fs quota terry pat
34% da quota usada.
85% da quota usada.
```

Exibindo a Quota e Outras Informações sobre um Volume

Emita o comando **fs listquota** para exibir as seguintes informações:

- O nome do volume que abriga cada arquivo ou diretório especificado
- A quota, expressa em números de quilobytes (`1024` indica um megabyte)
- O tamanho atual do volume (o número de quilobytes do atualmente usado)
- A porcentagem da quota usada
- A porcentagem de espaço usada na partição de disco que abriga o volume

A sintaxe do comando é a seguinte.

```
% fs listquota [<caminho do diretório/arquivo>+]
```

sendo que *caminho do diretório/arquivo* especifica o nome de caminho de um arquivo ou diretório em cada volume do qual serão exibidas informações da quota. Se você não fornecer um nome de caminho, a saída relatará as informações da quota de volume que contém o diretório do trabalho atual.

Exemplo: Exibindo a Quota e Outras Informações sobre um Volume

O exemplo a seguir exibe as informações da quota sobre o volume que abriga o diretório de origem do usuário **terry**.

```
% fs listquota ~terry
Nome do Volume  Quota    Usada      % Usada     Partição
user.terry      10000    3400       34%         86%
```

Exibindo a Quota e Outras Informações sobre um Volume e Partição

Emita o comando **fs examine** para exibir as seguintes informações sobre um volume e a partição em que ele está localizado:

- O número de ID do volume (abreviado na saída como `vid`)
- O nome do volume

- O tamanho atual e a quota de volume, em quilobytes
- O número de blocos de quilobyte disponíveis na partição de disco que abriga o volume e o tamanho total dessa partição
- Uma *mensagem off-line* associada ao volume, se houver, conforme definição de um administrador do sistema

A sintaxe do comando é a seguinte.

```
% fs examine [<caminho do diretório/arquivo>+]
```

sendo que *caminho do diretório/arquivo* especifica o nome de caminho de um arquivo ou diretório em cada volume do qual serão exibidas informações da quota. Se você não fornecer um nome de caminho, a saída relatará as informações da quota de volume que contém o diretório do trabalho atual.

Exemplo: Exibindo a Quota e Outras Informações sobre um Volume e Partição

O exemplo a seguir exibe a quota e outras informações sobre o volume que abriga o diretório de trabalho atual.

```
% fs examine
Status do volume de vid = 536871122 named user.terry
A quota de disco atual é 10000
Os blocos atuais usados são 5745
A partição tem 1593 blocos disponíveis dentre 99162
```

Localizando Arquivos e Diretórios

Normalmente, não é preciso saber qual máquina servidor de arquivos armazena o volume que contém um arquivo ou diretório. Dado o nome de caminho a um arquivo, o Gerenciador de Cache da máquina cliente acessa automaticamente a máquina servidor apropriada.

Se você não conseguir acessar um arquivo, entretanto, ele poderá ser útil para que você saiba qual máquina servidor de arquivos o abriga. Você poderá então verificar se a máquina ou o processo do Servidor de Arquivos está funcionando corretamente, conforme descrita em “Verificando o Status das Máquinas do Servidor” na página 28. Ou, se os administradores do sistema programarem um tempo de inatividade para uma máquina, você poderá saber se a queda de energia será capaz de evitar que você acesse certos arquivos.

Exibindo a Localização de um Arquivo ou de um Diretório

Emita o comando **fs whereis** para exibir a máquina servidor de arquivos em que um arquivo ou diretório foi armazenado.

```
% fs whereis [<caminho do diretório/arquivo>+]
```

sendo que *caminho do diretório/arquivo* especifica o nome de caminho de cada arquivo ou diretório do qual serão exibidas as informações de localização. Se

você não fornecer um nome de caminho, a saída relatará a máquina que abriga o volume que contém o diretório de trabalho atual.

Se a saída mencionar mais de uma máquina, haverá uma cópia do volume em cada site (o volume será *replicado*). Os administradores do sistema podem escolher replicar os volumes que contêm informações que muitas pessoas precisam usar, tanto por razões de balanceamento de carga, quanto para tornar as informações disponíveis mesmo que haja uma queda de energia em uma máquina que abriga o volume.

Exemplo: Exibindo a Localização do Diretório

O exemplo a seguir exibe os nomes das máquinas do servidor que abrigam os volumes pessoais dos usuários **terry** e **pat**.

```
% cd /afs/abc.com/usr
% fs whereis terry pat
O arquivo /afs/abc.com/usr/terry está no host fs2.abc.com
O arquivo /afs/abc.com/usr/pat está no host fs3.abc.com
```

Verificando o Status das Máquinas do Servidor

·s vezes uma ou mais máquinas do servidor na célula tornam-se inacessíveis devido a problemas de hardware, de software ou, manutenção de rotina. Durante a queda de energia, você não pode acessar os arquivos armazenados nessas máquinas ou salvar as alterações feitas nos arquivos que estão armazenados nelas. (Seu Gerenciador de Cache possivelmente tem cópias dos arquivos armazenados localmente, com os quais você ainda pode trabalhar.)

Para verificar o status das máquinas do servidor, use o comando **fs checkservers**. Se a máquina de um servidor tiver mais do que um endereço da interface de rede (for *multihome*), o Gerenciador de Cache enviará a mensagem de verificação do status a todas as interfaces da máquina. Se pelo menos uma das interfaces do servidor responder, a saída do comando descreverá a máquina como acessível. Caso não haja resposta de nenhuma das interfaces, a saída descreverá a máquina como inacessível, mas exibirá somente uma das interfaces (geralmente aquela com a melhor posição de desempenho; consulte "Exibindo a Classificação por Preferência do Servidor" na página 30).

Para verificar o status de grupos diferentes de máquinas do servidor, combine as opções do comando **fs checkservers** como indicado:

- Para verificar as máquinas do servidor de arquivos na célula local somente, não inclua nenhuma opção.
- Para verificar as máquinas do servidor de arquivos somente em uma determinada célula externa, inclua o argumento **-cell**.
- Para verificar cada máquina servidor de arquivos que o Gerenciador de Cache contatou em qualquer célula, inclua o sinalizador **-all**.

Pode levar alguns minutos até que o prompt do shell de comando retorne, porque o interpretador de comandos **fs** aguarda um período de tempo antes de concluir que a máquina que não responde realmente não pode ser acessada. Para que o prompt do shell de comando retorne imediatamente, inclua o símbolo **&**, que executa o comando **fs checkservers** no segundo plano.

Verificando o Status da Máquina Servidor de Arquivos

Emita o comando **fs checkservers** para verificar o status das máquinas do servidor de arquivos.

```
% fs checkservers [-cell <célula para verificar>] [-all]  [&]
```

sendo que

-cell Nomeia cada célula na qual o status da máquina servidor será verificado. Não combine este argumento e o sinalizador **-all**.

-all Verifica o status de todas as máquinas do servidor. Não combine este sinalizador com o argumento **-cell**.

A mensagem a seguir indica que todas as máquinas do servidor responderam à mensagem de verificação de status do Gerenciador de Cache:

```
Todos os servidores estão em execução.
```

Caso contrário, uma mensagem como a seguinte listará as máquinas inacessíveis:

```
Estes servidores não estão disponíveis devido a problemas de
rede ou servidor: lista de máquinas.
```

Exemplo: Verificando o Status da Máquina Servidor

A mensagem a seguir verifica o status de cada máquina servidor de arquivos que o Gerenciador de Cache contatou em qualquer célula. Duas máquinas não estão respondendo.

```
% fs checkservers -all &
%Estes servidores estão indisponíveis devido a problemas
de rede ou servidor:
   fs1.abc.com server7.stateu.edu.
```

Determinando o Acesso a Células Externas

O Gerenciador de Cache mantém uma lista de células externas que ele sabe como alcançar. Uma célula deve aparecer na lista para que você tenha acesso a seus espaços de arquivos AFS. (Além disso, o ACL de cada diretório do nome de caminho do arquivo deve conceder a você as permissões necessárias, e o administrador do sistema deve montar a célula no espaço de arquivo AFS local—por convenção, somente no diretório **/afs**.)

Exibindo Células Externas

Emita o comando **fs listcells** para exibir as células que você pode acessar a partir desta máquina cliente. Pode levar alguns minutos até que o prompt do shell de comando retorne. O Gerenciador de Cache armazena as máquinas como endereços IP, mas estes são convertidos em nomes antes de serem exibidos. Para que o prompt do shell de comando retorne imediatamente, use o símbolo **&** para executar o comando **fs listcells** no plano de fundo como no exemplo a seguir.

```
% fs listcells &
%Célula abc.com em hosts
     db1.abc.com
     db2.abc.com
     db3.abc.com
Célula test.abc.com em hosts
     test4.abc.com.
Célula stateu.edu em hosts
     sv5.stateu.edu.
     sv2.stateu.edu.
     sv11.stateu.edu.
Célula def.com em hosts
     serverA.def.com
```

Exibindo a Classificação por Preferência do Servidor

O Gerenciador de Cache armazena uma lista de classificação das máquinas do servidor de arquivos. Quando ele precisa acessar um arquivo ou diretório, o Gerenciador de Cache compara as posições das máquinas do servidor de arquivos que abrigam o volume relevante. Ele primeiro tenta acessar o volume na máquina com a melhor classificação. (Se uma máquina servidor de arquivos for multihome—tiver mais do que uma interface de rede—o Gerenciador de Cache na verdade atribuirá posições separadas a cada interface.)

O Gerenciador de Cache atribui uma posição padrão a uma interface da máquina servidor de arquivos por meio da comparação do seu endereço IP com o endereço IP da interface. Ele atribui uma posição melhor às interfaces que estão em sua própria sub-rede ou rede do que às interfaces de outras redes. Por isso, as posições influenciam o Gerenciador de Cache a buscar os arquivos das máquinas do servidor de arquivos que estão próximas em termos da distância da rede, o que tende a reduzir o tráfego da rede e ajudar o Gerenciador de Cache a distribuir os dados às aplicações mais rapidamente.

O Gerenciador de Cache armazena cada posição como um par do endereço IP de uma interface da máquina servidor de arquivos e um número inteiro da posição entre o intervalo de **0** a **65.534**. Um número menor é uma posição melhor. Para exibir as posições de preferência do servidor na máquina cliente local, use o comando **fs getserverprefs**.

O Gerenciador de Cache armazena um conjunto de posições separado mas similar para os Servidores Volume Location (VL), o que informa ao Gerenciador de Cache a localização dos volumes que abrigam arquivos e diretórios. Para exibir essas posições, inclua o sinalizador **-vlservers** no comando **fs getserverprefs**.

Se as posições padrão não parecerem resultar em desempenho melhor, o administrador do sistema poderá alterá-las. Pergunte ao administrador do sistema sobre as posições se for apropriado.

Exibindo Posições de Preferência do Servidor

Emita o comando **fs getserverprefs** para exibir as posições de preferência da máquina servidor de arquivos usadoss pelo Gerenciador de Cache na máquina local. Para exibir as posições do Servidor VL, inclua o sinalizador **-vlservers**. Por definição, o Gerenciador de Cache tem o endereço IP de cada interface convertido em um nome de host antes de sua exibição. Para ignorar a conversão e exibir os endereços IP, inclua o sinalizador **-numeric**. Isso pode aumentar significativamente a velocidade de saída do comando.

```
% fs getserverprefs [-numeric] [-vlservers]
```

O exemplo a seguir exibe as posições de preferência da máquina servidor de arquivos de uma máquina cliente na célula **abc.com**. As posições das máquinas servidor de arquivos dessa célula são inferiores àquelas das máquinas do servidor de arquivos da célula externa, **def.com**. Em razão do sinalizador **-numeric** não ser usado, a saída exibe os nomes de host. A aparência de um endereço IP das duas máquinas indica que a conversão delas não foi possível.

```
% fs getserverprefs
fs2.abc.com         20007
fs3.abc.com         30002
fs1.abc.com         20011
fs4.abc.com         30010
server1.def.com     40002
192.12.105.34       40000
server6.def.com     40012
192.12.105.37       40005
```

Capítulo 4. Protegendo Seus Diretórios e Arquivos

Este capítulo explica como proteger os arquivos e diretórios AFS por meio da definição das permissões em uma lista de controle de acesso.

Listas de Controle de Acesso

O AFS amplia e aprimora o esquema UNIX padrão de controle do acesso aos arquivos e diretórios. Ao invés de usar bits de modo para definir as permissões de acesso a arquivos separados, como o UNIX faz, o AFS armazena uma *lista de controle de acesso* (Acess Control List *ACL*) com cada diretório. Ele define quais usuários e grupos podem acessar o diretório e os arquivos que ele contém e de que maneira podem fazê-lo. Um ACL pode armazenar cerca de 20 entradas, cada uma delas com um usuário ou grupo e um conjunto de permissões. O AFS define sete permissões em lugar das três que o UNIX usa.

Um outro aprimoramento ao esquema de proteção UNIX padrão é o de que os usuários podem definir *grupos* de proteção próprios e depois posicionar os grupos em ACLs como se eles fossem usuários individuais. Um grupo pode incluir tanto usuários, quanto máquinas. Cada usuário que pertence a um grupo herda todas as permissões concedidas ao grupo no ACL. Da mesma forma, todos os usuários que estão conectados à uma máquina que pertence a um grupo herdam todas as permissões concedidas ao grupo. Você pode criar grupos para posicionar em ACLs e também usar grupos que outros usuários tenham criado. Para aprender mais sobre a criação de grupos, consulte “Capítulo 5. Utilizando Grupos” na página 51.

Além disso, o AFS define dois grupos de sistemas chamados **system:anyuser** e **system:authuser**. Ao colocá-los em ACLs, você pode conceder acesso a um grande número de usuários de uma vez. Consulte “Utilizando os Grupos do Sistema em ACLs” na página 37.

Embora o AFS use ACLs para proteger arquivos e diretórios, ele também usa os bits de modo UNIX para uma extensão limitada. Consulte “Como o AFS Usa os Bits de Modo UNIX” na página 48.

Controle de Acesso no Nível do Diretório

Conforme foi descrito, o AFS associa um ACL a cada diretório, e ele se aplica a todos os arquivos armazenados no diretório. Os arquivos não têm ACLs separados. A definição do acesso no nível do diretório tem diversas conseqüências:

- As permissões do ACL de um diretório se aplicam a todos os arquivos do diretório. Quando você desloca um arquivo para um diretório diferente, você efetivamente altera suas permissões para as do ACL de seu novo diretório. A mudança do ACL de um diretório altera a proteção de todos os arquivos dele.
- Quando você cria um subdiretório, ele herda o ACL atual de seu diretório pai. Você pode definir o ACL do subdiretório diferentemente do de seu diretório pai. Entretanto, não torne o ACL do diretório pai mais restritivo do que o de um subdiretório, porque isso pode evitar que os usuários acessem o subdiretório mesmo quando eles tiverem as permissões necessárias de seu ACL. Especificamente, um usuário deve ter a permissão **l** (**lookup** - busca), definida em "As Permissões ACL AFS", no diretório pai para chegar aos seus subdiretórios.

Como uma regra geral, faz sentido conceder um acesso completamente liberal ao diretório de origem. Se você precisar proteger certos arquivos mais de perto, coloque-os em subdiretórios que têm ACLs mais restritivas.

As Permissões ACL AFS

Existem sete permissões ACL AFS padrão. Funcionalmente, elas se encaixam em dois grupos: um que se aplica ao diretório em si e outro que se aplica aos arquivos.

As Quatro Permissões do Diretório

As quatro permissões deste grupo são significativas em relação ao diretório em si. Por exemplo, a permissão **i** (**insert** - inserção) não controla a inclusão de dados em um arquivo, mas a criação de um novo arquivo ou subdiretório.

A permissão l (lookup - procurar)

Esta permissão funciona como um gerenciador de acesso ao diretório e seus arquivos, porque o usuário deve possui-la a fim de empregar qualquer outra permissão. Em particular, o usuário deve ter essa permissão para acessar qualquer coisa nos subdiretórios do diretório.

Esta permissão possibilita que o usuário emita os seguintes comandos:

- O comando **ls** para listar os nomes dos arquivos e subdiretórios do diretório
- O comando **ls -ld** para obter informações completas do status do elemento do diretório em si
- O comando **fs listacl** para examinar o ACL do diretório

Esta permissão não possibilita que o usuário leia o conteúdo de um arquivo no diretório ou emita os comandos **ls -l** ou **fs listacl** com um nome de arquivo como o argumento. Estas operações requerem a permissão **r** (**read** - leitura), que está descrita em "As Três Permissões do Arquivo" na página 35.

Da mesma forma, esta permissão não possibilita que um usuário emita os comandos **ls**, **ls -l**, **ls -ld** ou **fs listacl** em relação a um subdiretório do diretório. Estas operações requerem a permissão **l** no ACL do, subdiretório próprio.

A permissão i (insert - inserir)
Esta permissão possibilita que o usuário inclua novos arquivos no diretório, por criação ou cópia, e crie novos subdiretórios. Ela não se estende a nenhum subdiretório que se encontra protegido por seus ACLs.

A permissão d (delete - excluir)
Esta permissão possibilita que o usuário remova arquivos e subdiretórios do diretório ou desloque-os para outros diretórios (admitindo que o usuário tenha a permissão **i** no ACL dos outros diretórios).

A permissão a (administer - administrar)
Esta permissão possibilita que o usuário altere o ACL do diretório. Os membros do grupo **system:administrators** implicitamente têm esta permissão em cada diretório (ou seja, mesmo se esse grupo não aparecer no ACL). Da mesma forma, o proprietário de um diretório implicitamente tem esta permissão no ACL e em todos aqueles diretórios abaixo dele.

As Três Permissões do Arquivo

As três permissões deste grupo são significativas em relação aos arquivos de um diretório, e não em relação ao diretório em si ou seus subdiretórios.

A permissão r (read - ler)
Esta permissão possibilita que o usuário leia o conteúdo dos arquivos do diretório e emita o comando **ls -l** para iniciar os elementos do arquivo.

A permissão w (write - gravar)
Esta permissão possibilita que o usuário modifique o conteúdo dos arquivos do diretório e emita o comando **chmod** para alterar seus bits de modo UNIX.

A permissão k (lock - bloquear)
Esta permissão possibilita que o usuário execute programas que emitem chamadas do sistema para bloquear arquivos no diretório.

As Oito Permissões Auxiliares

O AFS fornece oito permissões adicionais que não têm um significado definido. Elas são indicadas pelas letras maiúsculas **A**, **B**, **C**, **D**, **E**, **F**, **G** e **H**.

O administrador do sistema pode escolher gravar os programas de aplicação que atribuam um significado a uma permissão ou mais, e depois colocá-los

em ACLs para controlar o acesso ao arquivo por esses programas. Use os comandos **fs listacl** e **fs setacl** para exibir e definir as permissões auxiliares em ACLs exatamente como as sete padrão.

Notação Reduzida dos Conjuntos de Permissões

Você pode combinar as sete permissões de qualquer modo em uma entrada ACL, mas certas combinações são mais úteis do que outras. Quatro das combinações mais comuns têm formas reduzidas correspondentes. Ao utilizar o comando **fs setacl** para definir as entradas ACL, você pode fornecer uma ou mais letras separadas que representem as permissões, ou uma das seguintes formas reduzidas:

all Representa as sete permissões padrão (**rlidwka**)

none Remove a entrada do ACL, deixando o usuário ou grupo sem nenhuma permissão

read Representa as permissões **r** (**read** - ler) e **l** (**lookup** - procurar)

write Representa todas as permissões exceto **a** (**administer** - administrar): **rlidwk**

Considerações Sobre as Permissões Normais e de Negação

Os ACLs possibilitam que você conceda e negue acesso a um diretório e aos arquivos nele contidos. Para conceder acesso, use o comando **fs setacl** para criar uma entrada ACL que associa um conjunto de permissões a um usuário ou grupo, conforme descrito em “Alterando um ACL” na página 41. Quando você usa o comando **fs listacl** para exibir um ACL (conforme descrito em “Exibindo um ACL” na página 39), tais entradas aparecem sob o seguinte cabeçalho, que usa o termo *direitos* para se referir às permissões:

```
Direitos normais
```

Existem dois modos de negar acesso:

1. O método recomendado é o de simplesmente omitir uma entrada do usuário ou grupo do ACL, ou omitir as permissões apropriadas de uma entrada. Use o comando **fs setacl** para remover ou editar uma entrada existente. Na maioria dos casos, este método é suficiente para evitar acesso de certos tipos ou por certos usuários. Você deve ter cuidado, porém, para não conceder as permissões indesejadas a algum grupo ao qual tais usuários pertencem.
2. O método mais explícito de negar acesso é posicionar uma entrada na seção *permissões negativa* de um ACL, por meio da inclusão do sinalizador **-negative** no comando **fs setacl**. Para obter instruções, consulte “Incluindo, Removendo ou Editando as Permissões Negativas do ACL” na página 43. O comando **fs listacl** exibe a seção permissões negativas de um ACL sob o seguinte cabeçalho:

   ```
   Direitos de negação
   ```

Ao determinar qual tipo de acesso será concedido a um usuário, o AFS primeiro examina todas as entradas na seção permissões normais do ACL. Depois, ele subtrai todas as permissões associadas ao usuário (ou aos grupos aos quais o usuário pertence) da seção permissões negativas do ACL. Por isso, as permissões negativas sempre cancelam as permissões normais.

As permissões negativas podem ser confusas, porque elas invertem o significado usual do comando **fs setacl**. Em particular, a combinação da redução **none** e do sinalizador **-negative** é uma negação dupla: por meio da remoção de uma entrada da seção permissões negativas do ACL, você possibilita que o usuário obtenha mais uma vez as permissões através das entradas na seção permissões normais. A combinação da redução **all** com o sinalizador **-negative** nega explicitamente todas as permissões.

É inútil criar uma entrada na seção permissões negativas se uma entrada na seção permissões normais conceder as permissões negativas ao grupo **system:anyuser**. Nesse caso, os usuários podem obter as permissões simplesmente por meio da utilização do comando **unlog** que descarta seus tokens. Quando eles fizerem isso, o AFS os reconhecerá como o usuário **anônimo**, que pertence ao grupo **system:anyuser**, mas não coincide com as entradas da seção permissões negativas do ACL.

Definindo ACLs DFS

Se a sua máquina estiver configurada para acessar o espaço de arquivo DFS de uma célula DCE através do AFS/DFS Migration Toolkit, você poderá usar os comandos do AFS **fs listacl** e **fs setacl** para exibir e definir os ACLs em diretórios e arquivos DFS que você possui. Porém, o DFS usa um conjunto de permissões ligeiramente diferente e uma sintaxe diferente para as entradas ACL. Consulte a documentação DFS ou pergunte ao administrador do sistema.

Utilizando os Grupos do Sistema em ACLs

O AFS define dois *grupos do sistema* que concedem acesso a um grande número de usuários de uma vez quando posicionado em um ACL. Porém, você não pode controlar os membros destes grupos, portanto considere cuidadosamente que tipo de permissões deseja lhes conceder. (Você deve controlar os membros dos grupos que você mesmo possui; consulte "Capítulo 5. Utilizando Grupos" na página 51.)

system:anyuser
: Inclui qualquer um que possa acessar a árvore de arquivos da célula, incluindo usuários que têm tokens na célula local, usuários que foram conectados em uma máquina cliente AFS local, mas não obtiveram tokens (tais como o superusuário local **root**), e usuários que estavam conectados à uma máquina local de fora da célula. A criação de uma

entrada ACL deste grupo é o único modo de estender o acesso aos usuários AFS das células externas, a menos que o administrador do sistema crie contas de autenticação local para eles.

system:authuser
Inclui todos os usuários que têm um token AFS válido, obtido do serviço de autenticação AFS da célula local.

O terceiro grupo do sistema, **system:administrators**, inclui um pequeno grupo de administradores que têm permissões extensivas na célula. Você geralmente não precisa colocar esse grupo em ACLs, porque seus membros sempre têm a permissão **a** (**administer** - administrar) em cada ACL, mesmo se o grupo não aparecer nele.

Ativando o Acesso aos Subdiretórios

Um usuário deve ter a permissão **l** a um diretório para acessar seus subdiretórios de qualquer modo. Mesmo se os usuários tiverem permissões extensivas em um subdiretório, eles não poderão acessá-lo se o ACL do diretório pai não conceder a permissão **l**.

Você pode conceder a permissão **l** de uma destas três formas: a um grupo do sistema (**system:anyuser** ou **system:authuser**), a usuários separados ou a um ou mais grupos de usuários definidos por você ou por outros usuários (consulte “Capítulo 5. Utilizando Grupos” na página 51). A concessão da permissão **l** ao grupo **system:anyuser** é a opção mais fácil e geralmente a mais segura porque a permissão apenas possibilita que os usuários listem o conteúdo do diretório, não leiam os arquivos dele. Se você quiser possibilitar somente que usuários localmente autenticados listem o conteúdo de um diretório, substitua o grupo **system:authuser** pelo grupo **system:anyuser**. O administrador do sistema possivelmente já criou uma entrada no ACL do seu diretório de origem que concede as permissões **r** e **l** ao grupo **system:anyuser**.

Estendendo o Acesso aos Processos do Serviço

·s vezes é necessário conceder permissões mais extensas ao grupo **system:anyuser** para que os processos que fornecem o serviço de entrega de correspondência e impressão possam funcionar corretamente. Por exemplo, os processos de impressão às vezes precisam da permissão **r** além da permissão **l**. Um processo de entrega de correspondência possivelmente precisa da permissão **i** para posicionar novas mensagens no diretório de correspondência. O administrador do sistema provavelmente já criou as entradas ACL necessárias. Se você notar uma entrada ACL que não possui um propósito claro, confira com o administrador do sistema antes de removê-la.

Estendendo o Acesso aos Usuários de Células Externas

O único modo de conceder acesso aos usuários das células externas que não têm uma conta na célula é colocar o grupo **system:anyuser** em um ACL.

Lembre-se, porém, que tal entrada estende o acesso a qualquer um que possa alcançar a célula, não apenas aos usuários AFS das células externas que você tem em mente.

Exibindo um ACL

Para exibir o ACL associado a um arquivo ou diretório, emita o comando **fs listacl**.

Nota aos usuários do AFS/DFS Migration Toolkit: Se a máquina da qual você emite o comando **fs listacl** estiver configurada para acessar o espaço de arquivo DFS de uma célula DCE através do AFS/DFS Migration Toolkit, você poderá usar o comando para exibir o ACL em arquivos e diretórios DFS. Para exibir o Initial Container ou o Initial Object ACL de um diretório DFS em lugar do regular, inclua o sinalizador **-id** ou **-if** do comando **fs listacl**. Para obter mais informações, pergunte ao administrador do sistema. O interpretador do comando **fs** ignora os sinalizadores **-id** e **-if** se você os incluir ao exibir um ACL AFS.

Exibindo um ACL

1. Emita o comando **fs listacl**.

```
% fs listacl [<caminho do diretório/arquivo>+]
```

sendo que

la
: É um alias aceitável do **listacl** (e **lista** é a menor abreviatura aceitável).

caminho do diretório/arquivo
: Nomeia um ou mais arquivos ou diretórios dos quais será exibido o ACL. Para um arquivo, a saída exibe o ACL em seu diretório. Se você omitir este argumento, a saída será destinada ao diretório de trabalho atual. Os nomes de caminhos parciais são interpretados em relação ao diretório de trabalho atual. Você também pode usar a seguinte notação independentemente ou como parte de um nome de caminho:

  . (Um único ponto). Especifica o diretório de trabalho atual.

  .. (Dois pontos). Especifica o diretório pai do diretório de trabalho atual.

  ***** (O asterisco). Especifica cada arquivo e subdiretório do diretório de trabalho atual. O ACL exibido para um arquivo é sempre igual ao de seu diretório, mas o ACL de cada subdiretório pode variar.

A saída de cada arquivo ou diretório especificada como *caminho do diretório/arquivo* começa com o seguinte cabeçalho que a identifica:

```
A lista de acesso do caminho do diretório/arquivo é
```

O cabeçalho `Direitos normais` aparece na próxima linha, seguido por linhas cada uma com um usuário ou nome de grupo e um conjunto de permissões. As permissões aparecem como as únicas letras definidas em “As Permissões ACL AFS” na página 34, e sempre na ordem **rlidwka**. Se houver alguma permissão de negação, o cabeçalho `Direitos de negação` aparece depois, seguido pelos pares das permissões negativa.

Se aparecer esta mensagem de erro em lugar de um ACL, você não terá as permissões necessárias para exibir um ACL. Para especificar o nome de um diretório como o argumento *caminho do diretório/arquivo*, você deverá ter a permissão **l** (**lookup** - procurar) no ACL. Para especificar o nome de um arquivo, você deverá também ter a permissão **r** (**read** - ler) no ACL de seu diretório.

```
fs: Você não tem as permissões de acesso necessárias em
'caminho do diretório arquivo'
```

Exemplo: Exibindo o ACL em Um Diretório

O exemplo a seguir exibe o ACL no diretório de origem do usuário **terry** da célula ABC Corporation:

```
% fs la /afs/abc.com/usr/terry
A lista de acesso do /afs/abc.com/usr/terry é
Direitos normais:
   system:authuser rl
   pat rlw
   terry rlidwka
Direitos de negação:
   terry:other-dept rl
   jones rl
```

sendo que **pat**, **terry** e **jones** são usuários individuais, **system:authuser** é um grupo do sistema e **terry:other-dept** é um grupo a que **terry** pertence. A lista de permissões normais concede todas as permissões a **terry**, as permissões **rlw** a **pat** e as permissões **rl** aos membros do grupo **system:authuser**.

A lista de permissões negativas nega as permissões **rl** a **jones** e aos membros do grupo **terry:other-dept**. Essas entradas efetivamente evitam que eles acessem o diretório de origem do **terry** de qualquer modo; elas cancelam as permissões **rl** estendidas ao grupo **system:authuser**, que é a única entrada na seção permissões normais do ACL que possivelmente se aplica a eles.

Exemplo: Exibindo os ACLs em Vários Diretórios

O exemplo a seguir ilustra como você pode especificar nomes de caminhos de diferentes modos, e a aparência da saída dos vários diretórios. Ele exibe o ACL dos três diretórios: o diretório de trabalho atual (que é um subdiretório do diretório de origem do usuário **terry**), o diretório de origem do usuário **pat** e um outro subdiretório do diretório de origem de **terry** chamado **plans**.

```
% fs listacl  .  /afs/abc.com/usr/pat  ../plans
A lista de acesso de . é
Direitos normais:
   system:anyuser rl
   pat:dept rliw
A lista de acesso de /afs/abc.com/usr/pat é
Direitos normais:
   system:anyuser rl
   pat rlidwka
   terry rliw
A lista de acesso de ../plans é
Direitos normais:
   terry rlidwka
   pat rlidw
```

Alterando um ACL

Para incluir, remover ou editar entradas ACL, use o comando **fs setacl**. Por definição, o comando manipula as entradas na seção permissões normais do ACL. Para manipular as entradas na seção permissões negativa, inclua o sinalizador **-negative** seguindo as instruções relacionas em “Incluindo, Removendo ou Editando as Permissões Negativas do ACL” na página 43.

Você pode alterar qualquer ACL em que você já tenha a permissão **a**. Você sempre tem a permissão **a** no ACL de cada diretório que possui, mesmo se você acidentalmente tenha removido essa permissão do ACL. (O comando **ls -ld** informa o proprietário de um diretório.) O administrador do sistema normalmente designa você como proprietário do diretório de origem e seus subdiretórios, e você possivelmente possui outros diretórios também.

Se já existe uma entrada ACL para o usuário ou grupo especificado, as novas permissões substituirão completamente as permissões existentes e não serão acrescentadas a elas. Em outras palavras, ao emitir o comando **fs setacl**, você deverá incluir todas as permissões que deseja conceder a um usuário ou grupo.

Nota aos usuários do AFS/DFS Migration Toolkit: Se a máquina da qual você emite o comando **fs setacl** estiver configurada para acessar o espaço de arquivo DFS de uma célula DCE através do AFS/DFS Migration Toolkit, você poderá usar o comando para definir o ACL em arquivos e diretórios DFS. Para definir o Initial Container ou o Initial Object ACL de um diretório DFS em lugar do regular, inclua o sinalizador **-id** ou **-if** do comando **fs setacl**. Para obter mais informações, pergunte ao administrador do sistema. O interpretador do comando **fs** ignora os sinalizadores **-id** e **-if** se você os incluir ao definir um ACL AFS.

Incluindo, Removendo ou Editando as Permissões ACL Normais

Emita o comando **fs setacl** para editar entradas na seção permissões normais do ACL. Para remover uma entrada, especifique a redução **none** como as permissões. Se já existir uma entrada ACL para um usuário ou grupo, as permissões especificadas substituirão completamente aquelas da entrada existente.

```
% fs setacl  -dir <diretório>+ -acl <lista de entrada de acesso>+
```

sendo que

sa É um alias aceitável do **setacl** (e **seta** é a menor abreviatura aceitável).

-dir Nomeia um ou mais diretórios aos quais serão aplicadas as entradas ACL definidas pelo argumento **-acl**. Os nomes de caminhos parciais são interpretados em relação ao diretório de trabalho atual. Você também pode usar a seguinte notação independentemente ou como parte de um nome de caminho:

. (Um único ponto). Se usado sozinho, define o ACL no diretório de trabalho atual.

.. (Dois pontos). Se usado sozinho, define o ACL no diretório pai do diretório de trabalho atual.

***** (Asterisco). Define o ACL em cada um dos subdiretórios do diretório de trabalho atual. Ele deve ser precedido pelo comutador **-dir**, já que potencialmente ele designa diversos diretórios. O interpretador de comandos **fs** gera a seguinte mensagem de erro para cada arquivo do diretório:

```
fs: 'nome de arquivo': Não é um diretório
```

Se você especificar somente o nome de um diretório (ou arquivo), poderá omitir os comutadores **-dir** e **-acl**. Para obter outras informações sobre a omissão dos comutadores, consulte "Apêndice B. Sintaxe do Comando e Ajuda Online AFS" na página 79.

-acl Especifica uma ou mais entradas ACL, cada uma delas com o nome de um grupo ou usuário e um conjunto de permissões. Separe os pares e as duas partes de cada par com um ou mais espaços.

Para definir as permissões, forneça:

- Uma ou mais das letras que representam as permissões auxiliares ou padrão (**rlidwka** e **ABCDEFGH**), em qualquer ordem
- Uma das quatro notações reduzidas:
  - **all** (iguala **rlidwka**)
  - **none** (remove a entrada)
  - **read** (iguala **rl**)

– **write** (iguala **rlidwk**)

Em uma única linha de comandos, você pode combinar as entradas do usuário e grupo. Pode também combinar letras individuais e usar as notações reduzidas, mas não dentro de um único par.

Exemplo: Incluindo uma Única Entrada ACL

Um dos comandos do exemplo a seguir concede ao usuário **pat** as permissões **r** e **l** no ACL do subdiretório **notes** do diretório de trabalho atual. Eles ilustram como é possível omitir os comutadores **-dir** e **-acl** quando você nomear somente um diretório.

```
% fs sa notes pat rl
% fs sa pat read
```

Exemplo: Definindo Várias Entradas ACL em Um Diretório

O exemplo a seguir edita o ACL do diretório de trabalho atual. Ele remove a entrada do grupo **system:anyuser**, e inclui duas entradas: uma concede todas as permissões exceto **a** aos membros do grupo **terry:colleagues** e a outra concede as permissões **r** e **l** ao grupo **system:authuser**.

```
% fs sa  -dir . -acl  system:anyuser none  terry:colleagues write  \
          system:authuser rl
```

Incluindo, Removendo ou Editando as Permissões Negativas do ACL

Emita o comando **fs setacl** com o sinalizador **-negative** para editar as entradas na seção permissões negativas do ACL. Para remover uma entrada, especifique a redução **none** como as permissões. Se já existir uma entrada ACL para um usuário ou grupo, as permissões especificadas substituirão completamente aquelas da entrada existente.

```
% fs setacl  -dir <diretório>+ -acl <lista de entrada de acesso>+  -negative
```

sendo que

sa
: É um alias aceitável do **setacl** (e **seta** é a menor abreviatura aceitável).

-dir
: Nomeia um ou mais diretórios aos quais serão aplicadas as entradas negativas do ACL definidas pelo argumento **-acl**. Para obter uma descrição detalhada dos valores aceitáveis, consulte "Incluindo, Removendo ou Editando as Permissões ACL Normais" na página 42.

-acl
: Especifica uma ou mais entradas ACL, cada uma delas com o nome de um grupo ou usuário e um conjunto de permissões. Separe os pares, e as duas partes de cada par, com um ou mais espaços. Para obter uma descrição detalhada dos valores aceitáveis, consulte "Incluindo, Removendo ou Editando as Permissões ACL Normais" na página 42. Lembre-se de que o significado usual de cada permissão será invertido.

-negative
: Posiciona as entradas definidas pelo argumento **-acl** na seção permissões negativas do ACL de cada diretório nomeado pelo argumento **-dir**.

Exemplo: Definindo uma Entrada na Seção Permissões Negativas

O usuário **terry** concedeu todas as permissões de acesso exceto **a** ao grupo **terry:team** em seu subdiretório **plans**.

```
% cd /afs/abc.com/usr/terry
% fs listacl plans
A lista de controle de acesso de plans é
Direitos normais:
   system:anyuser rl
   terry:team rlidwk
   terry  rlidwka
```

Porém, **terry** observa que um dos membros do grupo, o usuário **pat**, fez alterações inadequadas nos arquivos. Para evitar que isso ocorra sem remover o **pat** do grupo ou sem alterar as permissões do grupo **terry:team**, **terry** cria uma entrada na seção permissões negativas do ACL que nega as permissões **w** e **d** ao **pat**:

```
% fs setacl plans pat wd -negative
% fs listacl plans
A lista de controle de acesso de plans é
Direitos normais:
   system:anyuser rl
   terry:team rlidwk
   terry: rlidwka
Direitos de negação:
   pat wd
```

Exemplo: Restaurando o Acesso pela Remoção de uma Entrada da Seção Permissões Negativa

No exemplo anterior, o usuário **terry** coloca **pat** na seção permissões negativas do ACL para o subdiretório **plans**. Mas o resultado foi inconveniente e **pat** prometeu não alterar mais os arquivos. Para possibilitar que **pat** exercite todas as permissões concedidas aos membros do grupo **terry:team**, **terry** remove a entrada de **pat** da seção permissões negativas do ACL.

```
% fs setacl plans pat  none -negative
% fs listacl plans
A lista de controle de acesso de plans é
Direitos normais:
   system:anyuser rl
   terry:team rlidwk
   terry  rlidwka
```

Substituindo Completamente um ACL

·s vezes, é mais simples limpar um ACL completamente antes de definir novas permissões nele, por exemplo, se a variedade de permissões normais e de negação tornar difícil de entender como sua interação afeta o acesso ao diretório. Para limpar um ACL completamente enquanto define novas entradas, inclua o sinalizador **-clear** no comando **fs setacl**. Quando você inclui esse sinalizador, pode criar entradas na seção permissões normais ou permissões negativas do ACL, mas não em ambas as seções de uma vez.

Lembre-se de criar uma entrada você mesmo. Como proprietário do diretório, você sempre precisará da permissão **a** (**administer** - administrar) na substituição de uma entrada excluída, mas os efeitos de uma entrada ACL ausente podem ser confusos o bastante para tornar difícil de perceber que o problema é a falta de uma entrada. Em particular, a falta da permissão **l** (**lookup** - procurar) evita que você use qualquer notação reduzida em nomes de caminhos (tais como um ponto para o diretório de trabalho atual e dois pontos para o diretório pai).

Substituindo um ACL Completamente

Emita o comando **fs setacl** com o sinalizador **-clear** para limpar o ACL completamente antes de definir as permissões normais ou de negação. Em razão de você precisar conceder ao proprietário do diretório todas as permissões, é melhor, na maioria dos casos, definir permissões normais neste ponto.

```
% fs setacl  -dir <diretório>+ -acl <lista de entrada de acesso>+ -clear
  [ -negative]
```

sendo que

sa É um alias aceitável do **setacl** (e **seta** é a menor abreviatura aceitável).

-dir Nomeia um ou mais diretórios aos quais serão aplicadas as entradas ACL definidas pelo argumento **-acl**. Para obter uma descrição detalhada dos valores aceitáveis, consulte “Incluindo, Removendo ou Editando as Permissões ACL Normais” na página 42.

-acl Especifica uma ou mais entradas ACL, cada uma delas com o nome de um grupo ou usuário e um conjunto de permissões. Separe os pares, e as duas partes de cada par, com um ou mais espaços. Lembre-se de conceder todas as permissões ao proprietário do diretório. Para obter uma descrição detalhada dos valores aceitáveis, consulte “Incluindo, Removendo ou Editando as Permissões ACL Normais” na página 42.

-clear Remove todas as entradas de cada ACL antes de criar as entradas indicadas pelo argumento **-acl**.

-negative
Posiciona as entradas definidas pelo argumento **-acl** na seção permissões negativas de cada ACL.

Exemplo: Substituindo o ACL

O seguinte exemplo limpa o ACL no diretório de trabalho atual e cria entradas que concedem todas as permissões ao usuário **terry** e todas as permissões exceto **a** ao usuário **pat**.

```
% fs setacl . terry all pat write -clear
% fs listacl .
A lista de controle de acesso de . é
Direitos normais:
  terry rlidwka
  pat rlidwk
```

Copiando ACLs Entre Diretórios

O comando **fs copyacl** copia o ACL de um diretório de origem para um ou mais diretórios de destino. Ele, na verdade, não afeta o ACL de origem, mas altera cada ACL de destino da seguinte forma:

- Se uma entrada do ACL de origem não existir no ACL de destino, o comando copia a mesma para o ACL de destino.
- Se uma entrada do ACL de destino também não existir no ACL de origem, o comando não a remove, a menos que você inclua o sinalizador **-clear**, que substitui o ACL de destino completamente.
- Se uma entrada estiver em ambos os ACLs, o comando altera a entrada do ACL de destino para que coincida com a entrada ACL de origem.

Para copiar um ACL, é preciso ter a permissão **l** no ACL de origem e a permissão **a** em cada ACL de destino. Se você identificar o diretório de origem pela nomeação de um arquivo nele, precisará também ter a permissão **r** no ACL de origem. Para exibir as permissões que você possui nos dois diretórios, use o comando **fs listacl** conforme descrito em “Exibindo um ACL” na página 39.

Nota aos usuários do AFS/DFS Migration Toolkit: Se a máquina da qual você emite o comando **fs copyacl** estiver configurada para acessar o espaço de arquivo DFS de uma célula DCE através do AFS/DFS Migration Toolkit, você poderá usar o comando para copiar ACLs entre arquivos e diretórios DFS também. O comando inclui os sinalizadores **-id** e **-if** para a alteração dos ACLs do Initial Container e do Initial Object de um diretório DFS, assim como a de seu ACL regular; para obter os detalhes, pergunte ao administrador do sistema. Você não pode copiar ACLs entre os diretórios AFS e DFS, porque eles usam formatos ACL diferentes. O interpretador de comandos **fs** ignora os sinalizadores **-id** e **-if** se você os incluir ao copiar ACLs AFS.

Copiando um ACL Entre Diretórios

Emita o comando **fs copyacl** para copiar um ACL de origem para o ACL em um ou mais diretórios de destino.

```
% fs copyacl -fromdir <diretório fonte> -todir <diretório de destino>+  \
          [-clear]
```

sendo que

co É a menor abreviatura aceitável de **copyacl**.

-fromdir
Nomeia o diretório de origem do qual o ACL será copiado. Os nomes de caminhos parciais são interpretados em relação ao diretório de trabalho atual. Se este argumento nomear um arquivo, o ACL será copiado de seus diretórios.

-todir Nomeia cada diretório de destino para o qual o ACL de origem será copiado. Os nomes de caminhos parciais são interpretados em relação ao diretório de trabalho atual. Os nomes de arquivos não são aceitáveis.

-clear Substitui completamente o ACL de cada diretório de destino pelo ACL de origem.

Exemplo: Copiando um ACL de Um Diretório para Outro

Neste exemplo, o usuário **terry** copia o ACL de seu diretório de origem (o diretório de trabalho atual) para seu subdiretório **plans**. Ela começa pela exibição de ambos os ACLs.

```
% fs listacl . plans
A lista de acesso de . é
Direitos normais:
   terry rlidwka
   pat rlidwk
   jones rl
A lista de acesso de plans é
Direitos normais:
   terry rlidwka
   pat rl
   smith rl

% fs copyacl -from . -to plans

% fs listacl . plans
A lista de acesso de . é
Direitos normais:
   terry rlidwka
   pat rlidwk
   jones rl
A lista de acesso de plans é
Direitos normais:
```

```
terry rlidwka
pat rlidwk
jones rl
smith rl
```

Como o AFS Usa os Bits de Modo UNIX

Embora o AFS proteja os dados inicialmente com ACLs ao invés de bits de modo, ele não ignora os bits de modo inteiramente. Uma explicação de como os bits de modo funcionam no sistema de arquivos UNIX está fora do escopo deste documento, e as considerações a seguir pressupõe que você compreenda o funcionamento deles; se necessário, consulte a documentação do UNIX. Estas considerações também não tratam dos bits setuid, setgid ou sticky. Se você precisar saber como esses bits funcionam nos arquivos AFS, consulte o *AFS Administration Guide* ou peça ajuda ao administrador do sistema.

O AFS usa os bits de modo UNIX destas formas:

- Ele usa o bit inicial para distinguir arquivos e diretórios. Esse é o bit que aparece primeiro na saída do comando **ls -l** e mostra o hífen (**-**) de um arquivo ou a letra `d` de um diretório.
- Ele não usa nenhum dos bits de modo em um diretório. O ACL AFS sozinho controla o acesso ao diretório.
- Para um arquivo, o conjunto de bits do proprietário (primeiro) interage com as entradas ACL que se aplicam ao arquivo do seguinte modo. O AFS não usa o grupo ou mundo (segundo ou terceiro conjuntos) de bits de modo.
  - Se o primeiro bit de modo **r** não estiver definido, ninguém (incluindo o proprietário) poderá ler o arquivo, não importa que permissões eles tenham no ACL. Se o bit estiver definido, os usuários também precisarão das permissões **r** e **l** no ACL do diretório do arquivo para ler o arquivo.
  - Se o primeiro bit de modo **w** não estiver definido, ninguém (incluindo o proprietário) poderá modificar o arquivo. Se o bit **w** estiver definido, os usuários também precisarão das permissões **w** e **l** do ACL do diretório do arquivo para modificar o arquivo.
  - Não há nenhuma permissão ACL que corresponda diretamente ao bit de modo **x**, mas, para executar um arquivo armazenado em AFS, o usuário também precisará ter as permissões **r** e **l** no ACL do diretório do arquivo.

Quando você emitir o comando **chmod** UNIX em um arquivo ou diretório AFS, o AFS modificará os bits apropriadamente. Para alterar os bits de modo de um arquivo, é preciso ter a permissão **w** AFS no ACL do diretório do arquivo. Para alterar os bits de modo de um diretório, é preciso ter as permissões **d**, **i** e **l** em seu ACL.

Exemplo: Desativando o Acesso à Gravação de um Arquivo

Suponha que **terry** esteja presidindo um comitê que está desenvolvendo uma proposta. Conforme as seções são aprovadas, ela desativa o acesso à gravação desse arquivo para evitar outras alterações. Por exemplo, o comando **chmod** a seguir desativa os bits de modo **w** do arquivo **proposal.chap2**. Isso torna impossível que qualquer pessoa altere o arquivo, não importa que permissões foram concedidas no ACL do diretório.

```
% chmod -w proposal.chap2
% ls -l
-rw-r--r--  1 terry     573 Nov 10 09:57 conclusion
-r--r--r--  1 terry     573 Nov 15 10:34 intro
-r--r--r--  1 terry     573 Dez  1 15:07 proposal.chap2
-rw-r--r--  1 terry     573 Nov 10 09:57 proposal.chap3
-rw-r--r--  1 terry     573 Nov 10 09:57 proposal.chap4
```

Capítulo 5. Utilizando Grupos

Este capítulo explica como criar grupos e descreve diferentes formas de utilizá-los.

Sobre os Grupos

Um *grupo* do AFS é uma lista de usuários específicos que você pode colocar em listas de acesso de controle (ACLs). Os grupos tornam a manutenção dos ACLs muito mais fácil. Ao invés de criar uma entrada do ACL para cada usuário individualmente, você cria uma entrada para um grupo ao qual os usuários pertencem. Da mesma forma, você pode conceder a um usuário acesso a vários diretórios ao mesmo tempo, incluindo o usuário em um grupo que aparece nos ACLs relevantes.

As máquinas do cliente do AFS também podem pertencer a um grupo. Todos que estiverem conectados à máquina herdam as permissões concedidas ao grupo em um ACL, mesmo que não estejam autenticados com o AFS. Em geral, os grupos de máquinas são úteis apenas aos administradores do sistema, para fins específicos como satisfazer acordos de licença que sua célula tem com os fornecedores de software. Consulte o administrador do sistema antes de colocar uma máquina cliente em um grupo ou utilizar um grupo de máquinas em um ACL.

Para aprender sobre proteção de arquivos do AFS e como incluir grupos em ACLs, consulte “Capítulo 4. Protegendo Seus Diretórios e Arquivos” na página 33.

Sugestões para Utilizar Grupos com Eficiência

Há três formas comuns de se utilizar os grupos, cada uma adequada a um fim específico: uso privado, uso compartilhado e uso em grupo. Seguem abaixo sugestões apenas. Os grupos podem ser utilizados da forma como você desejar.

- *Uso privado*: você cria um grupo e coloca-o no ACL de diretórios que você possui, sem necessariamente informar os membros do grupo que eles pertencem a ele. Os membros apenas percebem que podem ou não acessar, de determinada forma, o diretório. Você possui controle administrativo exclusivo sobre o grupo, já que é o proprietário.

  A existência do grupo e a identidade de seus membros não são necessariamente secretos. Outros usuários podem ver o nome do grupo em um ACL quando utilizam o comando **fs listacl** e podem usar o comando **pts membership** para exibir + os grupos ao qual eles próprios pertencem.

No entanto, você pode limitar quem pode exibir os membros do grupo, como descrito em “Protegendo Informações Relacionadas ao Grupo” na página 63.

- *Uso compartilhado*: você informa aos membros do grupo que eles pertencem ao mesmo, mas você é o proprietário e administrador exclusivo do grupo. O gerenciador de um grupo de trabalho, por exemplo, pode criar um grupo de todos os membros no grupo de trabalho, e pode encorajá-los a utilizá-lo nas ACLs de diretórios que guardam informações que eles desejam compartilhar com outros membros do grupo.

  Nota: Se você colocar um grupo pertencente a outra pessoa em seus ACLs, o proprietário do grupo pode alterar a propriedade do grupo sem informá-lo. Uma pessoa pode ganhar ou perder acesso sem a sua interferência ou sem o seu conhecimento.
- *Uso em grupo*: você cria um grupo e depois utiliza o comando **pts chown** para atribuir propriedade a um grupo—outro grupo ou ao próprio grupo (o último é um grupo *auto-proprietário*). Você informa aos membros do grupo proprietário que eles podem administrar o grupo que possuem. Para obter instruções sobre o comando **pts chown**, consulte “Alterando o Proprietário de um Grupo” na página 61.

  A principal vantagem da designação de um grupo como proprietário é que várias pessoas compartilham a responsabilidade pela administração do grupo. Uma única pessoa não precisa executar todas as tarefas administrativas. Se o proprietário original do grupo deixar a célula, ainda existem outras pessoas que podem administrá-la.

  Entretanto, qualquer um no grupo proprietário pode fazer alterações que afetam negativamente os outros: incluir ou remover pessoas do grupo incorretamente ou alterar a propriedade do grupo exclusivamente para si mesmos. Estes problemas podem ser particularmente considerados em um grupo auto-proprietário. O uso de um grupo proprietário funciona melhor se todos os membros se conhecem e confiam uns nos outros; seria recomendável manter um número pequeno de pessoas em um grupo proprietário.

Nomes dos Grupos

Os grupos criados devem ter nomes com duas partes, no seguinte formato:

nome_do_proprietário:*nome_do_grupo*

O prefixo *nome_do_proprietário* indica qual usuário ou grupo possui o grupo (as regras de nomenclatura aparecem em “Criando um Grupo” na página 57). A parte *nome_do_grupo* indica a finalidade do grupo ou interesse comum de seus membros. Os nomes dos grupos sempre devem ser fornecidos por

completo, por isso um *nome_do_grupo* curto é mais prático. Entretanto, nomes como **terry:1** e **terry:2** não indicam que a finalidade do grupo seja menos útil do que nomes como **terry:project**.

Os grupos que não possuem o prefixo *nome_do_proprietário* possivelmente aparecem em alguns ACLs; eles são criados apenas pelos administradores do sistema. Todos os grupos que você cria devem ter um prefixo *nome_do_proprietário*.

Quota de criação de grupo

Por padrão, você pode criar 20 grupos, mas os administradores do sistema podem alterar sua *quota de criação de grupo*, se necessário. Quando você cria um grupo, sua quota tem um decréscimo de um. Quando um grupo criado é excluído, sua quota tem um acréscimo de um, mesmo que você não seja mais o proprietário. Você não pode aumentar sua quota transferindo a propriedade de um grupo para outra pessoa, porque você é sempre lembrado como o criador.

Se você esgotar sua quota de criação de grupo e precisar criar mais grupos, consulte o administrador do sistema. Para obter instruções sobre a exibição de sua quota de criação de grupo, consulte “Exibindo uma Entrada do Grupo” na página 55.

Exibindo Informações do Grupo

Você pode utilizar os seguintes comandos para exibir informações sobre os grupos e os usuários que pertencem a eles:

- Para exibir os membros de um grupo ou os grupos aos quais o usuário pertence, utilize o comando **pts membership**.
- Para exibir os grupos que um usuário ou grupo possui, utilize o comando **pts listowned**.
- Para exibir informações gerais sobre um usuário ou grupo, incluindo seu nome, ID do AFS, criador e proprietário, utilize o comando **pts examine**.

Nota: Os grupos do sistema **system:anyuser** e **system:authuser** não aparecem na lista de associações do grupo de um usuário e o comando **pts membership** não exibe seus membros. Para obter mais informações sobre grupos do sistema, consulte “Utilizando os Grupos do Sistema em ACLs” na página 37.

Exibindo as Associações do Grupo

Emita o comando **pts membership** para exibir os membros de um grupo ou os grupos aos quais um usuário pertence.

```
% pts membership <nome de usuário de grupo ou id>+
```

em que *usuário ou nome do grupo ou id* especifica o nome ou UID do AFS de cada usuário para o qual são exibidas as associações do grupo ou o nome ou GID do AFS de cada grupo para o qual são exibidas os membros. Se estiver identificando um grupo pela GID do AFS, preceda a GID com um hífen (**-**) para indicar que é um número negativo.

Exemplo: Exibindo os Membros de um Grupo

O exemplo abaixo exibe os membros do grupo **terry:team**.

```
% pts membership terry:team
Os membros do terry:team (id: -286) são:
  terry
  smith
  pat
  johnson
```

Exemplo: Exibindo os Grupos aos Quais um Usuário Pertence

O exemplo abaixo exibe os grupos aos quais os usuários **terry** e **pat** pertencem.

```
% pts membership terry pat
Grupos dos quais terry (id: 1022) é membro:
  smith:friends
  pat:accounting
  terry:team
Grupos dos quais pat (id: 1845) é membro:
  pat:accounting
  sam:managers
  terry:team
```

Exibindo os Grupos que um Usuário ou Grupo Possui

Emita o comando **pts listowned** para exibir os grupos que um usuário ou grupo possui.

```
%  pts listowned <usuário , nome do grupo ou id>+
```

em que *usuário, nome do grupo ou id* especifica o nome ou UID do AFS de cada usuário, ou o nome ou GID do AFS de cada grupo, para o qual são exibidas as posses do grupo. Se estiver identificando um grupo pela GID do AFS, preceda a GID com um hífen (-) para indicar que é um número negativo.

Exemplo: Exibindo os Grupos que um Grupo Possui

O exemplo abaixo exibe os grupos que o grupo **terry:team** possui.

```
% pts listowned -286
Os grupos que o terry:team (id: -286) possui são:
  terry:project
  terry:planners
```

Exemplo: Exibindo os Grupos que um Usuário Possui

O exemplo abaixo exibe os grupos que o usuário **pat** possui.

```
% pts listowned pat
Grupos que o pat (id: 1845) possui são:
   pat:accounting
   pat:plans
```

Exibindo uma Entrada do Grupo

Emita o comando **pts examine** para exibir informações gerais sobre um usuário ou grupo, incluindo seu nome, ID do AFS, criador e proprietário.

```
%  pts examine <usuário , nome do grupo ou id>+
```

em que *usuário, nome do grupo ou id* especifica o nome ou UID do AFS de cada usuário, ou o nome ou GID do AFS de cada grupo, para o qual são exibidas as informações relacionadas ao grupo. Se estiver identificando um grupo pela GID do AFS, preceda a GID com um hífen (**-**) para indicar que é um número negativo.

O resultado de saída inclui informações nos seguintes campos:

Nome
: Para os usuários, esta é a cadeia de caracteres digitada durante o login. Para as máquinas, o nome é o endereço IP; um zero no campo de endereço atua como um curinga, correspondente a qualquer valor. Para maioria dos grupos, este é um nome no formato *nome_do_usuário*:*nome_do_grupo*. Alguns grupos criados pelo administrador do sistema não possuem o prefixo *nome_do_proprietário*. Consulte “Nomes dos Grupos” na página 52.

id
: Este é um número de identificação exclusivo que os processos do servidor do AFS utilizam internamente. Sua função é semelhante a uma UID do UNIX, porém opera no AFS, ao contrário do sistema de arquivos UNIX. Os usuários e as máquinas possuem IDs de usuário (UIDs) do AFS com inteiros positivos, e os grupos possuem IDs de grupos do (GIDs) do AFS com inteiros negativos.

proprietário
: Este é o usuário ou grupo que possui a entrada e por isso pode administrá-la.

criador
: O nome do usuário que emitiu os comandos **pts createuser** e **pts creategroup** para criar a entrada. Este campo é útil principalmente como uma trilha de auditoria e não pode ser alterado.

associações
: Para os usuários e máquinas, ele indica a quantos grupos o usuário ou a máquina pertencem. Para os grupos, ele indica quantos membros pertencem ao grupo. Este número não pode ser definido explicitamente.

sinalizadores
Este campo indica quem pode relacionar determinadas informações sobre a entrada ou alterá-la de determinadas formas. Consulte "Protegendo Informações Relacionadas ao Grupo" na página 63.

quota do grupo
Este campo indica a quantidade de grupos que um usuário tem permissão para criar. Ele é definido em 20 quando a entrada do usuário é criada. A quota de criação para máquinas ou grupos é insignificante pois não é possível fazer a autenticação como um máquina ou grupo.

Exemplo: Listando Informações sobre um Grupo

O exemplo abaixo exibe informações sobre o grupo **pat:accounting**, que contém membros do departamento que o **pat** gerencia. Observe que o grupo é auto-proprietário, o que significa que todos os seus membros podem administrá-lo.

```
% pts examine pat:accounting
Nome: pat:accounting, id: -673, proprietário: pat:accounting, criador: pat,
  associações: 15, sinalizadores: S-M--, quota do grupo: 0
```

Exemplo: Listando Informações do Grupo sobre um Usuário

O exemplo abaixo exibe informações relacionadas ao grupo sobre o usuário **pat**. Os dois campos mais interessantes são `membros`, que mostra que o **pat** pertence a 12 grupos e `quota do grupo`, que mostra que o **pat** pode criar outros 17 grupos.

```
% pts examine pat
Nome: pat, id: 1045, proprietário: system:administrators, criador: admin,
  associações: 12, sinalizadores: S-M--, quota do grupo: 17
```

Criando Grupos e Incluindo Membros

Utilize o comando **pts creategroup** para criar um grupo e o comando **pts adduser** para incluir membros no mesmo. Os usuários e máquinas podem pertencer a grupos, mas outros grupos não.

Quando você cria um grupo, você normalmente torna-se proprietário dele automaticamente. Isto significa que pode administrá-lo sozinho: incluir e remover membros, alterar o nome do grupo, transferir a propriedade do grupo, ou excluir o grupo completamente. Se quiser, pode designar outro proprietário ao criar o grupo, incluindo o argumento **-owner** no comando **pts creategroup**. Quando se atribui propriedade a outro grupo, este grupo já deve existir e deve ter pelo menos um membro. Você também pode alterar a propriedade de um grupo após criá-lo utilizando o comando **pts chown** como descrito no "Alterando o Proprietário ou o Nome de um Grupo" na página 60.

Criando um Grupo

Emita o comando **pts creategroup** para criar um grupo. Sua quota de criação de grupo decresce em um para cada grupo.

```
% pts creategroup -name <nome do grupo>+ [-owner <proprietário do  grupo>]
```

em que

cg É uma alias para **creategroup** (e **createg** é a abreviação mais curta aceitável).

-name Nomeia cada grupo a ser criado. O nome deve ter o seguinte formato:

*nome_proprietário***:***nome_do_grupo*

O prefixo *nome_do_proprietário* deve indicar com precisão o proprietário do grupo. Por padrão, você é registrado como o proprietário e o *nome_do_proprietário* deve ser o seu nome de usuário do AFS. Você pode incluir o argumento **-owner** para designar outro usuário ou grupo do AFS como o proprietário, contanto que forneça o valor necessário no campo *nome_do_proprietário*:

- Se o proprietário for um usuário, ele deve ter o nome de usuário do AFS.
- Se o proprietário for outro grupo regular, ele deve corresponder ao campo *nome_do_proprietário* do grupo que o possui. Por exemplo, se o proprietário for o grupo **terry:associates**, o campo proprietário deve ser **terry**.
- Se o proprietário for um grupo sem um prefixo *nome_do_proprietário*, ele deve ter o nome do grupo que o possui.

O nome pode ter até 63 caracteres incluindo dois pontos. Utilize números e minúsculas, mas nenhum espaço ou caracteres de pontuação que não sejam dois pontos.

-owner

É opcional e atribui propriedade a um usuário que não seja você, ou a um grupo. Se você especificar um grupo, ele já deve existir e deve ter pelo menos um membro. (Isto significa que para transformar um grupo em auto-proprietário, você deve emitir o comando **pts chown** depois de usar este comando para criar o grupo, e o comando **pts adduser** para incluir um membro. Consulte "Alterando o Proprietário ou o Nome de um Grupo" na página 60.)

Não nomeie uma máquina como proprietária. Como ninguém pode fazer a autenticação como uma máquina, não há como administrar um grupo pertencente a uma máquina.

Exemplo: Criando um Grupo

No exemplo abaixo, o usuário **terry** cria um grupo para incluir todos os outros usuários em sua equipe de trabalho, e depois examina a nova entrada do grupo.

```
% pts creategroup terry:team
o grupo terry:team tem a id -286
% pts examine terry:team
Nome: terry:team, id: -286, proprietário: terry, criador: terry,
  associações: 0, sinalizadores: S----, quota do grupo: 0.
```

Incluindo Membros em um Grupo

Emita o comando **pts adduser** para incluir um ou mais usuários em um ou mais grupos. Você sempre pode incluir membros em um grupo que possui (diretamente ou por pertencer ao grupo). Quando você pertence a um grupo, você pode incluir membros se o quarto sinalizador de privacidade for a letra minúscula **a**; consulte "Protegendo Informações Relacionadas ao Grupo" na página 63.

```
% pts adduser -user <nome do usuário>+ -group <nome do grupo>+
```

Você deve se incluir em grupos que você possui, se for adequado. Você não pertence a eles automaticamente somente por possuir o grupo.

Nota: Caso você já tenha um token ao ser incluído em um grupo, você deve emitir o comando **klog** para efetuar a re-autenticação antes de poder exercer as permissões concedidas ao grupo nas ACLs.

em que

-user
Especifica o nome de cada usuário a ser incluído nos grupos denominados pelo argumento **-group**. Os grupos não podem pertencer a outros grupos.

-group
Nomeia cada grupo para inclusão de usuários.

Exemplo: Incluindo Membros em um Grupo

Neste exemplo, o usuário **terry** inclui **pat**, **indira**, **smith** e a si mesmo no grupo que ele acabou de criar, **terry:team**, e depois verifica a nova lista de membros.

```
% pts adduser -user terry pat indira smith -group
terry:team
% pts members terry:team
Os membros do terry:team (id: -286) são:
  terry
  pat
  indira
  smith
```

Removendo Usuários de um Grupo ou Excluindo um Grupo

Você pode usar os seguintes comandos para remover grupos e seus membros:

- Para remover um usuário de um grupo, utilize o comando **pts removeuser**
- Para excluir completamente um grupo, utilize o comando **pts delete**
- Para remover grupos excluídos de ACLs, utilize o comando **fs cleanacl**

Quando um grupo que você criou é excluído, sua quota de criação de grupo aumenta em um, mesmo que você não possua mais o grupo.

Quando um grupo ou usuário é excluído, sua ID do AFS aparece nas ACLs em lugar do seu nome do AFS. Você pode usar o comando **fs cleanacl** para remover estas entradas obsoletas das ACLs em que você tem a permissão **a** (**administer**).

Removendo Membros de um Grupo

Emita o comando **pts removeuser** para remover um ou mais membros de um ou mais grupos. Você sempre pode remover membros de um grupo que seja seu (diretamente ou porque você pertence ao grupo de proprietários). Quando você pertence a um grupo, você pode remover membros se o quinto sinalizador de privacidade for a letra minúscula **r**; consulte “Protegendo Informações Relacionadas ao Grupo” na página 63. (Para exibir o proprietário de um grupo, utilize o comando **pts examine** como descrito em “Exibindo uma Entrada do Grupo” na página 55.)

```
% pts removeuser -user  <nome do usuário>+  -group <nome do grupo>+
```

em que

-user Especifica o nome de cada usuário a ser removido dos grupos denominados pelo argumento **-group**.

-group
Nomeia cada grupo a partir do qual deve-se remover usuários.

Exemplo: Removendo Membros do Grupo

O exemplo abaixo remove o usuário **pat** dos grupos **terry:team** e **terry:friends**.

```
% pts removeuser  pat -group terry:team terry:friends
```

Excluindo um Grupo

Emita o comando **pts delete** para excluir um grupo. Você sempre pode excluir um grupo que você possui (diretamente ou por pertencer ao grupo de proprietários). Para exibir o proprietário de um grupo, utilize o comando **pts examine** como descrito em “Exibindo uma Entrada do Grupo” na página 55.

```
% pts delete <usuário , nome do grupo ou id>+
```

em que *usuário, nome do grupo ou id* especifica o nome ou a UID do AFS de cada usuário, ou o nome ou GID do AFS de cada grupo, a ser excluído. Se

estiver identificando um grupo pela GID do AFS, preceda a GID com um hífen (**-**) para indicar que é um número negativo.

Exemplo: Excluindo um Grupo

No exemplo abaixo, o grupo **terry:team** é excluído.

```
% pts delete terry:team
```

Removendo Entradas Obsoletas do ACL

Emita o comando **fs cleanacl** para remover entradas obsoletas de ACLs depois que o usuário ou grupo correspondente tiver sido excluído.

```
% fs cleanacl [<caminho do diretório/arquivo>+]
```

em que *caminho do diretório/arquivo* nomeia cada diretório para o qual limpar o ACL. Se você omitir este argumento, o ACL do atual diretório de trabalho será limpo.

Exemplo: Removendo uma Entrada Obsoleta do ACL

Depois que o grupo **terry:team** é excluído, sua GID do AFS (-286) aparece em ACLs ao invés de seu nome. Neste exemplo, o usuário **terry** retira-o do ACL no diretório de planos em seu diretório de origem.

```
% fs listacl plans
A lista de acesso para planos é
Direitos normais:
  terry rlidwka
  -268 rlidwk
  sam rliw
% fs cleanacl plans
% fs listacl plans
A lista de acesso para planos é
Direitos normais:
  terry rlidwka
  sam rliw
```

Alterando o Proprietário ou o Nome de um Grupo

Para alterar o proprietário de um grupo, utilize o comando **pts chown**. Para alterar seu nome, utilize o comando **pts rename**.

Você pode alterar o proprietário ou nome de um grupo que você possui (diretamente ou por pertencer ao grupo de proprietários). Você pode atribuir a propriedade do grupo a outro usuário, outro grupo ou o próprio grupo. Caso ainda não seja um membro do grupo e precise ser, utilize o comando **pts adduser** antes de transferir a propriedade, seguindo as instruções em “Incluindo Membros em um Grupo” na página 58.

O comando **pts chown** altera automaticamente o prefixo *nome_do_proprietário* de um grupo para indicar o novo proprietário. Se o novo proprietário for um

grupo, apenas seu prefixo *nome_do_proprietário* é utilizado, não seu nome inteiro. No entanto, a alteração no comando do prefixo *nome_do_proprietário* não se propaga a nenhum grupo pertencente ao grupo cujo proprietário está sendo alterado. Se quiser que seus prefixos *nome_do_proprietário* indiquem o proprietário correto, você deve usar o comando **pts rename**.

Senão, você deve usar normalmente o comando **pts rename** para alterar apenas a parte *nome_do_grupo* de um nome do grupo (a parte que vêm após os dois pontos). Você pode alterar o prefixo *nome_do_proprietário* apenas para refletir o proprietário real.

Alterando o Proprietário de um Grupo

Emita o comando **pts chown** para alterar o nome de um grupo.

```
% pts chown  <nome do grupo> <proprietário novo>
```

em que

nome do grupo
: Especifica o nome atual do grupo ao qual atribuir um novo proprietário.

proprietário novo
: Nomeia o usuário ou grupo que irá possuir o grupo.

Exemplo: Alterando o Proprietário de um Grupo para Outro Usuário

No exemplo abaixo, o usuário **pat** transfere a propriedade do grupo **pat:staff** para o usuário **terry**. Seu nome muda automaticamente para **terry:staff**, como confirmado pelo comando **pts examine**.

```
% pts chown pat:staff terry
% pts examine terry:staff
Nome: terry:staff, id: -534, proprietário: terry, criador: pat,
  associações: 15, sinalizadores: SOm--, quota do grupo: 0.
```

Exemplo: Alterando o Proprietário de um Grupo para Si Mesmo

No exemplo abaixo, o usuário **terry** transforma o grupo **terry:team** em um grupo auto-proprietário. Seu nome não muda porque seu prefixo *nome_do_proprietário* já é **terry**.

```
% pts chown terry:team terry:team
% pts examine terry:team
Nome: terry:team, id: -286, proprietário: terry:team, criador: terry,
  associações: 6, sinalizadores: SOm--, quota do grupo: 0.
```

Exemplo: Alterando o Proprietário de um Grupo para um Grupo

Neste exemplo, o usuário **sam** transfere a propriedade do grupo **sam:project** para o grupo **smith:cpa**. Seu nome muda automaticamente para **smith:project**, pois **smith** é o prefixo *nome_do_proprietário* do grupo que agora o possui. O comando **pts examine** exibe o status do grupo antes e depois da alteração.

```
% pts examine sam:project
Nome: sam:project, id: -522, proprietário: sam, criador: sam,
  associações: 33, sinalizadores: SOm--, quota do grupo: 0.
% pts chown sam:project smith:cpa
% pts examine smith:project
Nome: smith:project, id: -522, proprietário: smith:cpa, criador: sam,
  associações: 33, sinalizadores: SOm--, quota do grupo: 0.
```

Alterando o Nome de um Grupo

Emita o comando **pts rename** para alterar o nome de um grupo.

```
% pts rename  <nome antigo> <nome atual>
```

em que

nome antigo
Especifica o nome atual do grupo.

nome novo
Especifica o nome novo completo a ser atribuído ao grupo. O prefixo *nome_do_proprietário* deve indicar corretamente o proprietário do grupo.

Exemplo: Alterando o Sufixo *nome_do_grupo* de um Grupo

O exemplo abaixo altera o nome do grupo **smith:project** para **smith:fiscal-closing**. O prefixo *nome_do_proprietário* do grupo permanece sendo **smith** porque seu proprietário não está sendo alterado.

```
% pts examine smith:project
Nome: smith:project, id: -522, proprietário: smith:cpa, criador: sam,
  associações: 33, sinalizadores: SOm--, quota do grupo: 0.
% pts rename smith:project smith:fiscal-closing
% pts examine smith:fiscal-closing
Nome: smith:fiscal-closing, id: -522, proprietário: smith:cpa, criador: sam,
  associações: 33, sinalizadores: SOm--, quota do grupo: 0.
```

Exemplo: Alterando o Prefixo *nome_do_proprietário* de um Grupo

Em um exemplo anterior, o usuário **pat** transferiu a propriedade do grupo **pat:staff** para o usuário **terry**. Seu nome mudou automaticamente para **terry:staff**. No entanto, um grupo que o **terry:staff** possui ainda chama-se **pat:plans**, porque a alteração no *nome_do_proprietário* de um grupo que resulta do comando **pts chown** não se propaga a nenhum grupo que ele possui. Neste exemplo, um membro de **terry:staff** utiliza o comando **pts rename** para alterar o nome para **terry:plans** para que reflita sua propriedade real.

```
% pts examine pat:plans
Nome: pat:plans, id: -535, proprietário: terry:staff, criador: pat,
  associações: 8, sinalizadores: SOm--, quota do grupo: 0.
% pts rename pat:plans terry:plans
% pts examine terry:plans
Nome: terry:plans, id: -535, proprietário: terry:staff, criador: pat,
  associações: 8, sinalizadores: SOm--, quota do grupo: 0.
```

Protegendo Informações Relacionadas ao Grupo

Os *sinalizadores de privacidade* de um grupo controlam quem pode administrá-lo de diversas formas. Os sinalizadores de privacidade aparecem no campo `sinalizadores` da saída a partir do comando **pts examine**; consulte “Exibindo uma Entrada do Grupo” na página 55. Para definir os sinalizadores de privacidade para um grupo que você possui, utilize o comando **pts setfields** como explicado em “Definindo os Sinalizadores de Privacidade de um Grupo” na página 64.

Interpretando os Sinalizadores de Privacidade

Os cinco sinalizadores de privacidade sempre aparecem, e sempre devem estar definidos, na seguinte ordem:

s Controla quem pode emitir o comando **pts examine** para exibir a entrada.

o Controla quem pode emitir o comando **pts listowned** para listar os grupos que um usuário ou grupo possui.

m Controla quem pode emitir o comando **pts membership** para listar os grupos aos quais um usuário ou grupo pertence ou quais usuários ou máquinas pertencem a um grupo.

a Controla quem pode emitir o comando **pts adduser** para incluir um usuário ou máquina em um grupo.

r Controla quem pode emitir o comando **pts removeuser** para remover um usuário ou máquina de um grupo.

Cada sinalizador pode receber três tipos de valores possíveis para permitir que um conjunto de usuários diferentes emita o comando correspondente:

- Um hífen (**-**) significa que o proprietário do grupo pode emitir o comando, juntamente com os administradores que pertencem ao grupo **system:administrators**.
- A versão em minúscula da letra significa que os membros do grupo podem emitir o comando, juntamente com os usuários indicados pelo hífen.
- A versão em maiúscula da letra significa que qualquer um pode emitir o comando.

Por exemplo, os sinalizadores `SOmar` em uma entrada do grupo indicam que qualquer um pode examinar a entrada do grupo e listar os grupos que ela possui, e que apenas os membros do grupo podem listar, incluir ou remover seus membros.

Os sinalizadores de privacidade padrão para os grupos são `S-M--`, isto é, qualquer um pode exibir a entrada e listar os membros do grupo, mas apenas o proprietário do grupo e os membros do grupo **system:administrators** podem realizar outras funções.

Definindo os Sinalizadores de Privacidade de um Grupo

Emita o comando **pts setfields** para definir os sinalizadores de privacidade em um ou mais grupos.

```
% pts setfields -nameorid <usuário , nome do grupo ou id>+
                -access <sinalizadores de privacidade de um grupo>
```

em que

-nameorid
Especifica o nome ou GID do AFS GID de cada grupo para o qual definir os sinalizadores de privacidade. Se estiver identificando um grupo pela GID do AFS, preceda a GID com um hífen (**-**) para indicar que é um número negativo.

-access
Especifica os sinalizadores de privacidade a serem definidos para cada grupo. Observe as seguintes regras:

- Forneça um valor para todos os cinco sinalizadores na ordem **somar**.
- Defina o primeiro sinalizador com **s** minúsculo ou **S** maiúsculo apenas.
- Defina o segundo sinalizador com o hífen (**-**) ou **O** maiúsculo apenas. Para os grupos, o AFS interpreta o hífen como equivalente ao **o** minúsculo (isto é, os membros de um grupo sempre podem listar os grupos que ele possui).
- Defina o terceiro sinalizador com o hífen (**-**), **m** minúsculo ou **M** maiúsculo.
- Defina o quarto sinalizador com o hífen (**-**), **a** minúsculo, ou **A** maiúsculo. O **A** maiúsculo não é uma opção segura, pois permite que qualquer pessoa inclua membros no grupo.
- Defina o quinto sinalizador com o hífen (**-**) ou **r** minúsculo apenas.

Exemplo: Definindo os Sinalizadores de Privacidade de um Grupo

O exemplo abaixo define os sinalizadores de privacidade no grupo **terry:team** para definir o padrão indicado de privilégio administrativo.

```
% pts setfields terry:team -access SOm--
```

- Qualquer pessoa pode emitir o comando **pts examine** para exibir informações gerais sobre ele (**S** maiúsculo).
- Qualquer pessoa pode emitir o comando **pts listowned** para exibir os grupos que ele possui (**O** maiúsculo).
- Os membros do grupo podem emitir o comando **pts membership** para exibir os membros do grupo (**m** minúsculo).

- Apenas o proprietário do grupo, o usuário **terry**, pode emitir o comando **pts adduser** para incluir membros (o hífen).
- Apenas o proprietário do grupo, o usuário **terry**, pode emitir o comando **pts removeuser** para remover membros (o hífen).

Capítulo 6. Detecção de problemas

Este capítulo explica como investigar e solucionar alguns problemas encontrados durante o trabalho com os arquivos AFS. Para usar as instruções, localize o título que descreve seu problema ou que coincide com a mensagem de erro recebida.

Problema: Impossível Acessar, Copiar ou Salvar Arquivo

1. Emita o comando **tokens** para verificar se possui tokens válidos. Para obter instruções completas, consulte “Exibindo Seus Tokens” na página 17.

   ```
   % tokens
   ```

   - Se os tokens forem válidos, passe para a etapa 2.
   - Caso você não tenha tokens para a célula relevante, ou eles tenham expirado, emita o comando **klog** para autenticar. Para obter instruções completas, consulte “Efetuando a Autenticação com o AFS” na página 16. Depois, tente acessar ou salvar o arquivo de novo. Se não for bem sucedido, continue na etapa 2.

     ```
     % klog
     ```

2. Emita o comando **fs checkservers** para verificar o status das máquinas do servidor de arquivos. Para obter instruções completas, consulte “Verificando o Status das Máquinas do Servidor” na página 28.

   ```
   % fs checkservers &
   ```

   - Se aparecer esta mensagem, passe para a etapa 3 na página 68.

     ```
     Todos os servidores estão em execução.
     ```

   - Uma saída como a seguinte indica que o Gerenciador de Cache não pode alcançar as máquinas do servidor de arquivos indicadas.

     ```
     Esses servidores estão indisponíveis devido a problemas de
     rede ou servidor: lista das mâquinas.
     ```

     Emita o comando **fs whereis** para verificar se o arquivo que você está tentando acessar ou salvar foi armazenado em uma das máquinas do servidor de arquivos inacessível. Para obter instruções completas, consulte “Localizando Arquivos e Diretórios” na página 27.

     ```
     % fs whereis <caminho do diretório/arquivo>
     ```

     Se o arquivo estiver armazenado em uma máquina inacessível, você não poderá acessar o arquivo ou salvá-lo novamente no Servidor de Arquivos até que a máquina esteja acessível novamente. Se o arquivo estiver em uma máquina que não está relacionada como inacessível, continue na etapa 3 na página 68.

3. Emita o comando **fs listacl** para verificar se tem as permissões necessárias para acessar, copiar ou salvar o arquivo. Para obter instruções completas, consulte “Exibindo um ACL” na página 39.

```
% fs listacl <caminho do diretório/arquivo>
```

Você precisa das permissões indicadas:

- Para acessar, copiar ou salvar um arquivo, você precisa ter a permissão **l** (**lookup** - procurar) no diretório e em todos os diretórios acima dele no nome do caminho.
- Para salvar as alterações de um arquivo existente, é preciso também ter a permissão **w** (**write** - gravar). Para criar um novo arquivo, é preciso também ter as permissões **i** (**insert** - inserir) e **w**.
- Para copiar um arquivo entre dois diretórios, é preciso ter a permissão **r** (**read** - ler) no diretório de origem e a permissão **i** no diretório de destino.

Se você não tiver as permissões necessárias mas possuir o diretório, sempre terá a permissão **a** (**administer** - administrar) mesmo se você não aparecer no ACL. Emita o comando **fs setacl** para conceder a si mesmo as permissões necessárias. Para obter instruções completas, consulte “Alterando um ACL” na página 41.

```
% fs setacl  -dir <diretório>+ -acl <accesso à lista de entradas>+
```

Se você não tiver as permissões necessárias e não possuir o diretório, peça ao proprietário ou ao administrador do sistema para concedê-las a você. Se eles incluírem você em um grupo que tem as permissões necessárias, você deverá emitir o comando **klog** para autenticar novamente antes de poder exercê-las.

Se você ainda não puder acessar o arquivo mesmo que tenha as permissões necessárias, entre em contato com o administrador do sistema para que ele ajude na investigação das possíveis causas do problema. Se você ainda não puder copiar ou salvar o arquivo mesmo que tenha as permissões necessárias, continue na etapa 4.

4. Se estiver copiando um arquivo, emita o comando **fs listquota** para verificar se o volume para o qual ele está sendo copiado, ou a partição que abriga esse volume, está quase cheia. Para o salvamento, verifique o volume e a partição que contém o diretório no qual você está salvando o arquivo. Para obter instruções completas, consulte “Exibindo a Quota de Volume” na página 25.

```
% fs listquota  <caminho do diretório /arquivo>
```

O comando produz a saída como no seguinte exemplo:

```
% fs listquota /afs/abc.com/usr/terry
Nome do Volume  Quota    Usada      % Usada     Partição
user.terry      10000    3400       34%         86%
```

- Se o valor do campo `Partição` não estiver próximo do 100%, a partição não estará quase cheia. Verifique o valor do campo `% Usado`. Se estiver próximo de 100%, o volume estará quase cheio. Se possível, exclua os arquivos que não são mais necessários do volume, ou peça que o administrador do sistema aumente a quota de volume.

  Se o valor do campo `% Usado` não estiver próximo de 100% (for, por exemplo, 90% ou menos), será improvável que você esteja excedendo a quota de volume, a menos que o arquivo seja muito grande ou a quota de volume muito pequena. Contate o administrador do sistema para obter ajuda na investigação das possíveis causas do problema.
- Se o valor do campo `Partição` estiver muito próximo a 100%, a partição possivelmente estará quase cheia. Porém, as partições da máquina de servidores geralmente são muito grandes e ainda têm espaço suficiente para um arquivo médio quando estão quase cheias. Você pode perguntar ao administrador do sistema sobre o status da partição ou emitir o comando **fs examine**. A linha final em sua saída relata quantos blocos de quilobytes ainda estão disponíveis na partição. Para obter instruções completas, consulte "Exibindo a Quota de Volume" na página 25.

  ```
  % fs examine  <caminho do diretório/arquivo>
  ```

  Se ainda houver espaço livre na partição, mas você ainda não puder salvar o arquivo, entre em contato com o administrador do sistema para que ele ajude na investigação das possíveis causas do problema.

Problema: Entrada Removida Acidentalmente de um ACL

1. Se você possuir o diretório do qual removeu acidentalmente sua entrada ACL, na verdade ainda terá a permissão **a** (**administer** - administrar) mesmo se ela não aparecer no ACL. Você normalmente possui o diretório de origem e todos seus subdiretórios, por exemplo. Emita o comando **fs setacl** para conceder a si mesmo todas as outras permissões. Para obter instruções completas, consulte "Incluindo, Removendo ou Editando as Permissões ACL Normais" na página 42.

   ```
   % fs setacl  -dir <diretório> -acl <seu_nome_do_usuário> all
   ```

   Para *diretório*, forneça o nome de caminho completo ao diretório (por exemplo: **/afs/abc.com/usr/***seu_nome_do_usuário*). Isso é necessário porque o AFS não pode interpretar as abreviaturas do nome de caminho se você não tiver a permissão **l** (**lookup** - procurar).
2. Caso você não tenha o diretório, emita o **fs listacl** para verificar se alguma entrada remanescente concede a você as permissões de que você precisa

(talvez você pertença a um ou mais grupos que aparecem no ACL). Para obter instruções completas, consulte “Exibindo um ACL” na página 39.

```
% fs listacl <caminho do diretório/arquivo>
```

- A seguinte mensagem exibe o ACL do diretório. Se você precisar de permissões que nenhuma entrada concede a você atualmente, peça ajuda ao proprietário do diretório ou ao administrador do sistema.

```
A lista de acesso de <caminho do diretório/arquivo> é
Direitos normais
lista de entradas
```

- Se o comando apresentar a seguinte mensagem de erro em lugar de um ACL, você não terá a permissão **l**.

```
fs: Você não tem os direitos de acesso necessários
em 'caminho do diretório/arquivo'.
```

  Peça ao proprietário do diretório ou ao administrador do sistema que conceda as permissões de que precisa. Se eles incluírem você em um grupo que tem as permissões necessárias, você deverá emitir o comando **klog** para autenticar novamente antes de poder exercê-las.

Mensagem de Erro: ″afs: Contato perdido com servidor de arquivos″

Emita o comando **fs checkservers** para verificar o status das máquinas do servidor de arquivos. Para obter instruções completas, consulte “Verificando o Status das Máquinas do Servidor” na página 28.

```
% fs checkservers &
```

- Se esta mensagem aparecer, peça ajuda ao administrador do sistema para diagnosticar a causa da mensagem de erro `Contato perdido`.

```
Todos os servidores estão em execução.
```

- Uma saída como a seguinte indica que o Gerenciador de Cache não pode alcançar as máquinas servidor de arquivos indicada. É preciso esperar até que eles estejam acessíveis novamente antes de continuar a trabalhar com os arquivos armazenados neles.

```
Esses servidores estão indisponíveis devido a problemas de rede ou servidor:
   lista_de_máquinas.
```

Mensagem de Erro: ″*command*: Tempo limite da conexão″

Emita o comando **fs checkservers** conforme descrito em “Mensagem de Erro: ″afs: Contato perdido com servidor de arquivos″”.

Mensagem de Erro: ″fs: Você não tem os direitos de acesso necessários no '*arquivo*'″

Você não tem as permissões ACL necessárias para a realização da operação que está tentando executar. Se possuir o diretório e tiver removido acidentalmente a si mesmo do ACL, consulte "Problema: Entrada Removida Acidentalmente de um ACL" na página 69. Caso contrário, peça ao proprietário do diretório ou ao administrador do sistema que conceda as permissões de que precisa.

Mensagem de Erro: ″afs: falha ao armazenar arquivo″

Siga as instruções em "Problema: Impossível Acessar, Copiar ou Salvar Arquivo" na página 67.

Apêndice A. Utilizando o NFS/AFS Translator

Algumas células utilizam o Network File System (NFS) em acréscimo ao AFS. Se você trabalha em uma máquina cliente do NFS, o administrador do sistema pode configurá-la para acessar o espaço de arquivo do AFS através de um programa chamado *NFS/AFS Translator*™. Se você possui uma conta do AFS, você pode acessar o AFS como um usuário autenticado enquanto estiver trabalhando em sua máquina cliente do NFS. Senão, você acessa o AFS como o usuário **anônimo**.

Nota: Um desempenho aceitável do NFS/AFS Translator requer que o NFS esteja funcionando corretamente.

Requisitos para Uso do NFS/AFS Translator

Para que você utilize o NFS/AFS Translator, o administrador do sistema deve configurar os seguintes tipos de máquinas conforme indicado:

- Uma máquina do *NFS/AFS translator* é uma máquina cliente do AFS que também atua como uma máquina servidor do NFS. Seu Gerenciador de Cache age como o Gerenciador de Cache substituto para sua máquina cliente do NFS. Pergunte ao administrador do sistema quais máquinas do translator você pode usar.
- Sua máquina cliente do NFS deve ter uma instalação do NFS para uma máquina do translator. Geralmente, o administrador do sistema instala o diretório **/afs** da máquina do translator e também atribui nome à instalação **/afs**. Isto permite ao usuário acessar o espaço de arquivo inteiro do AFS utilizando nomes de caminho padrão do AFS. Também é possível criar instalações diretamente em subdiretórios do **/afs** e atribuir à instalações do NFS nomes diferentes na máquina cliente do NFS.

Seu acesso ao AFS é muito mais amplo se você tiver uma conta de usuário do AFS. Caso não tenha, os servidores do AFS reconhecem você como usuário **anônimo** e concedem a você apenas o acesso disponível a membros do grupo **system:anyuser**.

Se a sua máquina cliente do NFS utiliza um sistema operacional que o AFS suporta, o administrador do seu sistema pode configurá-lo para permitir que você emita vários comandos do AFS na máquina. Pergunte a ele sobre a configuração e os comandos que você pode emitir.

Acessando o AFS através do Translator

Caso você não tenha uma conta do AFS ou opte por não acessar o AFS como um usuário autenticado, então tudo que você faz para acessar o AFS é fornecer o nome do caminho do arquivo relevante. O ACL deve conceder as permissões necessárias ao grupo **system:anyuser**.

Caso você tenha uma conta do AFS e deseje acessar o AFS como um usuário autenticado, o melhor método depende se sua máquina do NFS for um tipo suportado. Caso seja, utilize as instruções encontradas em "Efetuando a Autenticação em um Sistema Operacional Suportado". Se não for um tipo suportado, utilize as instruções encontradas em "Efetuando a Autenticação em um Sistema Operacional Não Suportado".

Efetuando a Autenticação em um Sistema Operacional Suportado

1. Efetue login na máquina cliente do NFS utilizando seu nome de usuário do NFS.
2. Emita o comando **klog**. Para obter instruções completas, consulte "Efetuando a Autenticação com o AFS" na página 16.

```
% klog -setpag
```

Efetuando a Autenticação em um Sistema Operacional Não Suportado

1. Efetue login na máquina cliente do NFS utilizando seu nome de usuário do NFS.
2. Estabeleça uma conexão com a máquina do NFS/AFS translator que você está utilizando (por exemplo, utilizando o utilitário **telnet**) e efetue login utilizando seu nome de usuário do AFS (que normalmente é o mesmo que seu nome de usuário do NFS).
3. Se a máquina do NFS/AFS translator utiliza um utilitário de login modificado pelo AFS, você terá obtido os tokens do AFS na Etapa 2. Para verificar, emita o comando **tokens**, descrito completamente em "Exibindo Seus Tokens" na página 17.

   ```
   % tokens
   ```

   Caso não possua tokens, emita o comando **klog**, descrito completamente em "Efetuando a Autenticação com o AFS" na página 16.

   ```
   % klog -setpag
   ```

4. Emita o comando **knfs** para associar seus tokens do AFS à sua UID do UNIX na máquina cliente do NFS em que está trabalhando. Isto permite que o Gerenciador de Cache na máquina do translator utilize os tokens adequadamente quando você acessa o AFS a partir da máquina cliente do NFS.

   Se à sua máquina cliente do NFS for um tipo de sistema para o qual o AFS define um nome de sistema, pode fazer sentido a inclusão do argumento **-sysname**. Este argumento ajuda o Gerenciador de Cache a

acessar binários específicos a sua máquina cliente do NFS, se o administrador do sistema tiver usado a variável *@sys* em nomes de caminho. Pergunte ao administrador do sistema se este argumento é útil para você.

```
% knfs <nome do host> [<ID do usuário (decimal)>]  \
       [-sysname <valor '@sys' do host>]
```

em que

nome do host
: Especifica o nome do host completamente qualificado de sua máquina cliente do NFS (tal como **nfs52.abc.com**).

ID do usuário
: Especifica sua UID do UNIX UID ou equivalente (não seu nome de usuário) na máquina cliente do NFS. Se o administrador do sistema tiver seguido o processo convencional, as UIDs do UNIX e do AFS serão iguais. Caso você não saiba qual é a sua UID local na máquina do NFS, peça ajuda ao administrador do sistema. O administrador do sistema também pode explicar os assuntos sobre os quais você deve estar ciente caso suas UIDs não sejam compatíveis ou caso você omita este argumento.

-sysname
: Especifica o nome do tipo de sistema da máquina cliente do NFS.

5. (**Opcional**) Efetue o logout da máquina do translator, mas não desfaça a autenticação.
6. Trabalhe na máquina cliente do NFS, acessando o AFS conforme necessário.
7. Ao terminar de acessar o AFS, emita o comando **knfs** na máquina do translator novamente. Forneça os mesmos argumentos *nome do host* e *ID do usuário* da Etapa 4 na página 74, e acrescente o sinalizador **-unlog** para destruir seus tokens. Se você efetuou o logout da máquina do translator na Etapa 5, primeiro você deve reestabelecer uma conexão com a máquina do translator como na Etapa 2 na página 74.

```
% knfs <nome do host> [<ID do usuário (decimal)>] -unlog
```

Detectando Problemas no NFS/AFS Translator

Um desempenho aceitável do NFS/AFS translator depende, em grande parte, do NFS. ·s vezes, os problemas que parecem ser períodos de inatividade do servidor de arquivos do AFS, conexões rompidas ou arquivos inacessíveis, na verdade são causados pelos períodos de inatividade do NFS.

Esta seção descreve alguns problemas comuns e suas possíveis causas. Se outros problemas surgirem, entre em contato com o administrador do sistema, que, se necessário, pode pedir ajuda ao grupo de Suporte do Produto do AFS.

Nota: Para evitar diminuir o desempenho do AFS, o Gerenciador de Cache na máquina do translator não envia imediatamente ao Servidor de Arquivos as alterações efetuadas nas máquinas do Cliente do NFS. Ao invés disso, ele verifica se há alterações a cada 60 segundos e depois as envia. Pode levar mais tempo para as alterações efetuadas em uma máquina cliente do NFS serem salvas do que para as alterações efetuadas em uma máquina cliente do AFS. A operação de salvamento deve ser concluída para que as alterações fiquem visíveis em máquinas cliente do NFS que estão utilizando uma máquina diferente do translator ou em máquinas cliente do AFS.

Sua Máquina Cliente do NFS está Pendente

Se o administrador do sistema tiver utilizado as opções recomendadas ao criar uma instalação do NFS para uma máquina do NFS/AFS translator, então a instalação será *permanente* e *poderá ser interrompida*:

- Uma instalação permanente significa que o cliente do NFS avalia os seus pedidos caso ele não receba uma resposta dentro do espaço de tempo esperado. Isto é útil porque os pedidos precisam passar pelo software do cliente do NFS e do AFS, o que algumas vezes pode levar mais tempo do que o esperado pelo cliente do NFS. No entanto, isto significa que se a máquina do NFS/AFS realmente tornar-se inacessível, a máquina cliente do NFS pode tornar-se inoperante (ficar *pendente* ou *interrompida*).
- Se a instalação do NFS puder ser interrompida, no caso de um período de inatividade da máquina do NFS/AFS translator, você pode pressionar <**Ctrl-c**> ou outro sinal de interrupção para descontinuar as tentativas repetidas do cliente do NFS em acessar o AFS. Então, pode continuar trabalhando localmente ou pode fazer uma instalação NFS de outra máquina do translator. Se a instalação do NFS não puder ser interrompida, você deve realmente remover a instalação para a máquina inacessível do translator.

Reinicializações do NFS/AFS Translator

Se você tiver feito a autenticação no AFS e a sua máquina do translator for reinicializada, você deve emitir o comando **klog** (e o comando **knfs**, quando apropriado) para efetuar a re-autenticação. Se utilizou o argumento **-sysname** do comando **knfs** para definir o nome do sistema de sua máquina cliente do NFS, utilize-o novamente.

Mensagens de Erro do Sistema

Esta seção explica os possíveis significados para as mensagens de erro do NFS que você recebe ao acessar o espaço de arquivo do AFS.

```
cliente do NFS danificado
```

```
Getpwd: não é possível ler
```

As duas mensagens possivelmente querem dizer que a sua máquina do translator foi reinicializada e não pode determinar o nome de caminho do atual diretório de trabalho. Para reestabelecer o caminho, altere o diretório e especifique o nome de caminho completo começando com **/afs**.

```
A máquina_translator do servidor do NFS não está respondendo,
ainda tentando.
```

O cliente do NFS não está recebendo uma resposta da máquina do NFS/AFS translator. Se a instalação do NFS para a máquina do translator for uma instalação permanente, o cliente do NFS continua tentando o pedido até obter uma resposta (consulte "Sua Máquina Cliente do NFS está Pendente" na página 76). Se a instalação do NFS para a máquina do translator for temporária, o cliente do NFS para de tentar após uma determinado número de tentativas (três, por padrão).

Apêndice B. Sintaxe do Comando e Ajuda Online AFS

Os comandos AFS disponíveis são usados na autenticação, na listagem de informações AFS, na proteção de diretórios, na criação e gerenciamento de grupos e na criação e gerenciamento de ACLs. Há três tipos gerais de comandos disponíveis a todos os usuários AFS: comandos do servidor de arquivos, comandos do servidor de proteção e comandos diversos. Este capítulo trata da sintaxe desses comandos AFS, das regras que devem ser seguidas na sua emissão e dos modos de acesso à ajuda relevante a eles.

Sintaxe do Comando AFS

A maioria dos comandos AFS usa a seguinte sintaxe:

```
command_suite operation_code -switch <valor>[+]  -flag
```

O *suíte de comando* indica o tipo geral de comando e o processo do servidor que executa o comando. Os usuários AFS regulares têm acesso a duas suítes de comandos principais e um conjunto de comandos diversos:

- A suíte de comandos **fs** é usada na emissão dos comandos do servidor de arquivos que interagem com o processo do Servidor de Arquivos.
- A suíte de comandos **pts** é usada na emissão dos comandos relacionados à proteção.
- Os comandos diversos não são associados a nenhuma suíte de comandos.

O *código de operação* indica a ação que o comando realiza. Os comandos diversos têm somente códigos de operação.

Um comando pode ter várias *opções*, que podem ser *argumentos* ou *sinalizadores*:

- Os argumentos são usados para fornecer informações adicionais a serem usadas pelo comando. Eles consistem no par *comutador* e *instância*. Um comutador define o tipo de argumento e é sempre precedido por um hífen; os argumentos podem ter várias instâncias se um sinal de mais (+) aparecer depois da instância. Uma instância representa alguma informação variável usada pelo comando. Os argumentos podem ser opcionais ou obrigatórios.
- Os sinalizadores são usados para orientar um comando a ser executado de um modo específico (por exemplo, para gerar um tipo de saída específico). Os sinalizadores sempre são precedidos por um hífen e são sempre opcionais.

Exemplo da Sintaxe do Comando

No seguinte comando AFS

```
% fs setacl -dir $HOME -acl pat all terry none -negative
```

- **fs** é a suíte de comandos.
- **setacl** é o *código de operações*, que orienta o processo do Servidor de Arquivos na definição de uma lista de controle de acesso.
- **-dir $HOME** e **-acl pat all terry none** são *argumentos*.
  - **-dir** e **-acl** são comutadores; **-dir** indica o nome do diretório em que o ACL será definido e **-acl** define as entradas para a definição dele.
  - **$HOME** e **pat all terry none** são *instâncias* dos argumentos. **$HOME** define um diretório específico para o argumento do diretório. O argumento **-acl** tem duas instâncias que especificam duas entradas ACL: **pat all** e **terry none**.
- **-negative** é um sinalizador, ele orienta o comando a colocar as entradas da lista de acesso no negativo, ao invés da lista de permissões normais.

Regras para o Uso dos Comandos AFS

Esta seção descreve as regras a serem seguidas na utilização dos comandos AFS.

Espaços e Linhas

Separe cada elemento de comando (suíte de comandos, código de operação, comutadores, instâncias e sinalizadores) com um espaço. Várias instâncias de um argumento também são separadas por um espaço.

Digite todos os comandos AFS em uma linha, seguidos por um retorno do carro. Alguns comandos deste documento aparecem em mais de uma linha, mas somente para legibilidade.

Abreviações e Aliases para Códigos de Operação

Você pode digitar códigos de operação de um dos três modos:

- Digitar o código de operação completo.
- Abreviar o código de operação para a forma mais curta que o distingue de outros códigos de sua suíte de comandos.
- Usar o alias do código de operação, se existir um.

Por exemplo, o comando **fs listacl** pode ser emitido assim:

- **fs listacl** (comando completo)
- **fs lista** (abreviação)
- **fs la** (alias)

O *AFS Administration Reference* fornece informações sobre a sintaxe dos comandos abreviados e completos, assim como todos os aliases dos comandos discutidos neste guia.

Omitindo Comutadores de Argumentos

Você pode omitir o comutador de um argumento se o comando tiver somente um argumento ou se as seguintes condições forem atendidas.

- Todos os argumentos necessários do comando aparecem na ordem prescrita pela instrução da sintaxe.
- Nenhum comutador é usado em qualquer argumento, mesmo se eles estiverem na ordem correta.
- Há somente um valor para cada argumento. A exceção importante dessa condição será se o argumento final necessário aceitar vários valores; nesse caso, é aceitável fornecer diversos valores sem fornecer o comutador.

Por exemplo, as dois comandos seguintes são equivalentes:

```
% fs setacl -dir /afs/abc.com/usr/terry/private -acl pat rl
% fs setacl /afs/abc.com/usr/terry/private pat rl
```

Porém, esta não é a forma reduzida aceitável porque os argumentos não estão na ordem prescrita:

```
% fs setacl -acl pat rl /afs/abc.com/usr/terry/private
```

Diminuindo Comutadores e Sinalizadores

Se for necessária a utilização de um comutador, ou se você decidir usar um sinalizador, poderá diminuir o nome desse comutador ou sinalizador contanto que a forma reduzida ainda seja distinta dos outros sinalizadores e comutadores do comando.

Por exemplo, ao emitir o comando **fs setacl**, você pode abreviar todos os comutadores e sinalizadores do comando para suas letras iniciais porque todos eles começam com uma letra diferente. Porém, ao emitir o comando **knfs**, o argumento **-host** e o sinalizador **-help** começam com a letra **h**, portanto as abreviaturas sem ambigüidades seriam **-ho** e **-he** respectivamente.

Diminuindo Referências ao Diretório

A maioria dos argumentos de comandos AFS que requerem instâncias de nomes de caminhos ou diretórios aceita uma ou mais destas formas reduzidas:

- Um único ponto (**.**) indica o diretório de trabalho atual.
- Dois pontos (**..**) indica o diretório pai do diretório de trabalho atual.
- A variável de ambiente $HOME indica o diretório de origem do emissor.

Por exemplo, se a usuária **terry** quiser conceder as permissões **r** (**read** - ler) e **l** (**lookup** procurar) em seu diretório de origem para sua gerente **pat**, **terry** poderá emitir este comando.

```
% fs setacl -dir $HOME -acl pat rl
```

Se o diretório de trabalho atual for o diretório de origem de **terry**, ela poderá emitir este comando.

```
% fs setacl -dir  .  -acl pat rl
```

Ambos os exemplos anteriores são formas reduzidas aceitáveis do comando:

```
% fs setacl -dir /afs/abc.com/usr/terry -acl pat rl
```

Comandos fs e pts Usados Normalmente

Esta seção fornece informações adicionais sobre os comandos **fs** e **pts** AFS geralmente usados. Para obter informações mais detalhadas, consulte o *AFS Administration Reference*.

Considerações sobre os Comandos fs

Alguns comandos **fs** estendem a semântica do sistema de arquivos UNIX por meio da solicitação das funções relacionadas ao arquivos que o UNIX não fornece (pela definição das listas de controle de acesso, por exemplo). Outros comandos **fs** ajudam a controlar o desempenho do Gerenciador de Cache em execução na máquina cliente local.

Todos os comandos **fs** aceitam o sinalizador **-help** opcional. Ele tem a mesma função do comando **fs help**: imprimir a mensagem de ajuda online de um comando da tela. Não forneça outras opções ao mesmo tempo que esse sinalizador. Ele as substitui, e o único efeito da emissão do comando será a exibição da mensagem de ajuda.

O privilégio necessário para a emissão dos comandos **fs** varia. Os privilégios necessários aos comandos **fs** descritos neste guia incluem estes:

- Ter certas permissões na lista de controle de acesso de um diretório. Por exemplo, a criação e remoção dos pontos de montagem requer as permissões **a** (**administer** - administrar, **i** (**insert** - inserir) e **d** (**delete** - excluir) do diretório no qual o ponto de montagem se localiza.
- Pertencer ao grupo **system:administrators** (consulte “Utilizando os Grupos do Sistema em ACLs” na página 37).
- Sem privilégio. Muitos comandos **fs** simplesmente listam as informações e portanto não requerem nenhum privilégio especial.

Considerações sobre os Comandos pts

A suíte de comandos **pts** é a interface através da qual se criam grupos de proteção e se incluem neles membros. Os administradores do sistema que pertencem a um grupo de sistema especial chamado **system:administrators** podem manipular qualquer grupo e também criar entradas da máquina e usuário que podem pertencer aos grupos. Os usuários que não pertencem ao

grupo **system:administrators** podem sempre listar as informações associadas às entradas do grupo que eles possuem, assim como as suas entradas de usuário. Dependendo da definição dos sinalizadores de privacidade de uma entrada, os usuários regulares podem às vezes acessar e manipular entradas do grupo de certas maneiras.

Todos os comandos **pts** aceitam argumentos e sinalizadores opcionais. Eles estão relacionados nas descrições do comando no *AFS Administration Reference* e estão descritos aqui em detalhes:

[-cell <*nome da célula***>]**
Este argumento indica que o comando é executado na célula indicada. O emissor pode abreviar o valor *nome da célula* para a menor forma que o distinga das outras células listadas no arquivo **/usr/vice/etc/CellServDB** da máquina cliente em que o comando foi emitido. Por definição, os comandos são executados na célula local conforme definido

- Primeiro, pelo valor da variável de ambiente AFSCELL. (Esta variável normalmente não se encontra definida. Se você estiver trabalhando em uma outra, célula não local por um período de tempo longo, poderá definir a variável como o nome dessa célula.)
- Segundo, no arquivo **/usr/vice/etc/ThisCell** da máquina cliente em que o comando é emitido.

[-force]
Este sinalizador orienta o interpretador de comando **pts** a continuar executando o comando, se possível, mesmo que ele encontre problemas durante a execução do comando. O interpretador de comandos executa o quanto for possível da operação solicitada, em vez de interrompê-la se encontrar um problema. O interpretador de comandos informa qualquer erro que encontrar durante a execução do comando. Esse sinalizador é especialmente útil se você fornecer muitas instâncias para um argumento; se uma das instâncias não for válida, o comando informará o erro e continuará com os argumentos restantes.

[-help]
Este sinalizador tem a mesma função do comando **pts help**: imprimir a mensagem de ajuda online de um comando da tela. Não forneça outras opções ao mesmo tempo que esse sinalizador. Ele as substitui, e o único efeito da emissão do comando será a exibição da mensagem de ajuda.

Obtendo Ajuda no AFS

A ajuda online do AFS consiste em mensagens de sintaxe básica. A distribuição AFS inclui uma ajuda em formato HTML que o administrador do sistema pode disponibilizar para você.

Exibindo Aliases e Sintaxe do Comando

Para exibir uma breve discussão de um comando, sua instrução de sintaxe e alias, caso haja, use o código de operação **help**. Por exemplo, para exibir a entrada da ajuda online do comando **fs listacl**, digite o comando:

```
% fs help listacl
fs listacl: lista de controle de acesso de listas
aliases: la
Uso: fs listacl  [-path <caminho do diretório/caminho>+]
[-id] [-if] [-ajuda]
```

Para exibir somente a instrução da sintaxe, use o sinalizador **-help**, disponível na maioria dos comandos AFS. Por exemplo, para exibir a instrução da sintaxe do comando **fs setacl**, digite o comando:

```
% fs setacl -help
Uso: fs setacl -dir <diretório>+ -acl <entradas de acesso de listas>+
[-limpar] [-negativa] [-id] [-if] [-ajuda]
```

Exibindo Descrições do Código de Operação

Para exibir uma breve descrição de todos os códigos de operação de uma suíte de comandos, emita o código de operação **help** sem nenhum outro argumento. Por exemplo, o comando **fs help** exibe uma breve descrição de cada código operacional na suíte de comandos **fs**.

Para exibir uma lista dos comandos em uma suíte de comandos relacionada a um certo tipo de objeto, forneça o argumento de uma palavra-chave relevante ao código de operação **apropos**. Por exemplo, se quiser definir um ACL, mas não conseguir se lembrar qual comando **fs** usar, emita o comando:

```
% fs apropos set
setacl: define uma lista de controle de acesso
setcachesize: define o tamanho do cache
setcell: define a célula de status
setclientaddrs: define os endereços de interface da rede de clientes
setquota: define a quota de volume
setserverprefs: define as posições dos servidores de arquivo
setvol: define o status de volume
sysname: obtém/define o valor (ex. @sys) do nome do sistema
```

A mensagem a seguir indica que não há nenhum comando cujos nomes ou descrições incluam a cadeia da palavra-chave fornecida:

```
Nenhum comando encontrado
```

Nota: Se a palavra-chave fornecida tiver espaços, coloque-a entre aspas duplas (″ ″).

Apêndice C. Glossário

Administrador do Sistema. Usuário autorizado a administrar uma célula do AFS.

Alias. Um nome alternativo para um comando do AFS.

Anônimo. A identidade atribuída a um usuário que não possui um token válido para a célula local.

Argumento. A parte de um comando que nomeia uma entidade para ser afetada pelo comando. Os argumentos são compostos por duas partes: uma *chave* e uma ou mais *instâncias*. Alguns comandos do AFS admitem um ou mais argumentos.

Arquivo. Um conjunto de informações armazenadas e recuperadas como uma unidade.

Arquivo no Cache. Uma cópia de um arquivo que o Gerenciador de Cache armazena no disco local de uma estação de trabalho.

Autenticação Mútua. Procedimento através do qual dois usuários comprovam identidades entre si. Os processos do servidor e do cliente do AFS geralmente autenticam-se mutuamente à medida que estabelecem uma conexão.

Autenticar. Ser reconhecido como um usuário válido do AFS através do fornecimento da senha correta. Faça a autenticação conectando-se à uma máquina que utiliza um utilitário de login modificado pelo AFS ou emitindo o comando **klog**. Apenas os usuários autenticados podem executar grande parte das ações do AFS.

Bits de Modo. Um conjunto de permissões que o sistema de arquivos UNIX associa a um arquivo ou diretório para controlar o acesso ao mesmo. Elas aparecem no primeiro campo da saída do comando **ls -l**.

Bits de Modo do UNIX. Veja a entrada **Bits de Modo**.

Byte, kilobyte. Unidades de medidas utilizada para medir o uso de espaço em um volume ou em uma partição. Um bloco de kilobyte é igual a 1024 bytes.

Callback. Uma garantia do Servidor de Arquivos em contatar o Gerenciador de Cache se a cópia do arquivo armazenada centralmente for alterada enquanto o Gerenciador de Cache possuir uma cópia no cache. Se o arquivo for alterado, o Servidor de Arquivos *rompe* o callback. A próxima vez que um programa de aplicação solicitar dados do arquivo, o Gerenciador de Cache observa o callback rompido e recupera do Servidor de Arquivos uma cópia atualizada do arquivo. Os callbacks asseguram que o usuário está trabalhando com a cópia mais recente de um arquivo.

Célula. Um site administrado independentemente operando o AFS, composto por um conjunto de máquinas do servidor de arquivos e máquinas do cliente definido para pertencer à célula. Uma máquina pode pertencer apenas a uma célula de cada vez.

Célula Externa. Uma célula diferente da célula à qual a máquina cliente pertence. Se a máquina cliente estiver configurada adequadamente, os usuários podem acessar o espaço de arquivo do AFS em células externas assim como a célula local, e podem fazer a autenticação em células externas nas quais tiverem contas do AFS.

Célula Local. A célula à qual pertence a conta do usuário e a máquina cliente.

Chave. Parte de uma cadeia de comandos que define o tipo de um argumento. Ela é precedida por um hífen.

Código de Operação. A segunda palavra em um comando do AFS que pertence a um conjunto. Ela indica a função do comando.

Comando. Uma cadeia de caracteres indicando uma ação a ser executada por um servidor do AFS. Para obter a descrição de uma sintaxe de comando do AFS, consulte "Apêndice B. Sintaxe do Comando e Ajuda Online AFS" na página 79.

Comandos Remotos. Comandos utilizados para executar programas em uma máquina remota sem estabelecer uma conexão persistente com ela.

Computação de Cliente/Servidor. Um sistema de computação no qual dois tipos de computadores (máquinas cliente e máquinas servidor) executam funções especializadas diferentes.

Conjunto de Comandos. Um grupo de comandos do AFS com funções relacionadas. O nome do conjunto de comandos é a primeira palavra em muitos dos comandos do AFS.

Conversor NFS/AFS. Programa que permite aos usuários em máquinas do cliente do NFS acessar arquivos no espaço de arquivo do AFS.

Diretório. Uma estrutura lógica que contém um conjunto de arquivos e outros diretórios.

Diretório de Origem. Diretório pertencente a um usuário e dedicado ao armazenamento dos arquivos pessoais do usuário.

Diretório Pai. O diretório no qual um diretório ou arquivo se localiza.

Entrada do ACL. Uma entrada em um ACL que emparelha um usuário ou grupo com permissões de acesso específicas.

Estrutura de Arquivos Hierárquica. Um método de armazenamento de dados em diretórios que são organizados em uma estrutura em árvore.

Gerenciador de Cache. Um conjunto de modificações feitas no sistema operacional em uma máquina cliente que permite aos usuários da máquina acessar arquivos armazenados no AFS. O Gerenciador de Cache solicita arquivos do Servidor de Arquivos e armazena (*coloca no cache*) uma cópia de cada arquivo no disco local da máquina cliente. Os programas da aplicação utilizam então a cópia colocada no cache, o que elimina os pedidos de rede repetidos para máquinas do servidor de arquivos.

Grupo. Uma lista definida de usuários, que pode ser colocada no ACL de um diretório para estender um conjunto de permissões a todos os seus membros de uma só vez.

Grupo auto-proprietário. Um grupo que é proprietário de si mesmo, permitindo que todos os seus membros o administrem.

Grupo pertencente a um Grupo. Um grupo pertencente a outro grupo. Todos os membros do grupo proprietário podem administrar o grupo que possuem; os membros do grupo que é possuído não tem permissão para sua auto-administração.

Grupos do Sistema. Grupos que o AFS define automaticamente para representar usuários que compartilham determinadas características. Veja as três entradas seguintes.

Grupo System:administrators. Grupo do sistema que contém usuários autorizados para administrar o AFS.

Grupo System:anyuser. Grupo do sistema que inclui todos que podem obter acesso ao espaço de arquivo do AFS da célula. Ele inclui usuários não-autenticados, que recebem a identidade **anônima**.

Grupo System:authuser. Grupo do sistema que inclui todos os usuários que, no momento, possuem tokens válidos do AFS para a célula local.

Instância. A parte de uma cadeia de comandos que define a entidade a ser afetada.

Instrução da Sintaxe. Especificação das opções disponíveis em um comando e sua classificação.

Kilobyte. Unidade de medida utilizada para medir o uso de espaço em um volume ou em uma partição. Um kilobyte é igual a 1024 bytes. O termo *bloco de kilobyte* é utilizado às vezes para se fazer referência ao espaço em disco.

Lista de Controle de Acesso (ACL). Uma lista associada a um diretório do AFS que especifica as ações que um usuário ou grupo pode executar no diretório e os arquivos nele contidos. Há sete permissões de acesso: **a** (**administrar**), **d** (**excluir**), **i** (**inserir**), **k** (**bloquear**), **l** (**procurar**), **r** (**ler**) e **w** (**gravar**).

Login. O processo de estabelecimento de uma conexão como um usuário específico ao sistema de arquivos local da máquina cliente.

Logout. O processo de término de uma conexão ao sistema de arquivos local.

Máquina do Servidor de Arquivos. Tipo de máquina que armazena arquivos e os transfere para máquinas do cliente através de pedidos.

Máquinas do Cliente. Computadores que fazem computações para os usuários. Os usuários geralmente trabalham em uma máquina cliente, acessando arquivos armazenados em uma máquina servidor de arquivos.

Nome de Caminho Completo. A especificação completa da localização de um arquivo no AFS, começando na raiz do espaço de arquivo (por convenção, instalada no diretório **/afs**) e especificando todos os diretórios pelos quais o Gerenciador de Cache deve passar para acessar o arquivo. Os nomes dos diretórios são separados por barras.

Nome de Caminho Relativo. Nome de caminho que não começa na raiz do AFS ou espaço de arquivo local e representa a localização de um arquivo ou diretório considerando o atual diretório de trabalho.

Nome do usuário. Uma cadeia de caracteres fornecida durante o login que identifica exclusivamente uma pessoa na célula local.

Partição. A seção lógica de um disco em um computador.

Permissão. Um determinado tipo de acesso concedido em um ACL. Qualquer um que tem a permissão pode executar a ação.

Permissão a (administrar). A permissão do ACL que permite ao proprietário alterar as entradas no ACL .

Permissão de bloqueio. Veja a entrada **Permissão k (bloquear)**.

Permissão d (excluir). A permissão do ACL que permite ao proprietário remover elementos de um diretório.

Permissão i (inserir). A permissão do ACL que permite ao proprietário incluir arquivos ou subdiretórios em um diretório.

Permissão k (bloquear). Veja a entrada Permissão k (bloquear). A permissão do ACL que permite que programas coloquem bloqueios de notificação em um arquivo.

Permissão l (procurar). A permissão do ACL que permite ao proprietário listar o conteúdo de um diretório e exibir seu ACL.

Permissão r (ler). A permissão do ACL que permite ao proprietário examinar o conteúdo de um arquivo.

Permissão w (gravar). A permissão do ACL que permite ao proprietário modificar o conteúdo de um arquivo.

Ponto de Instalação. Um tipo especial de diretório que associa uma localização no espaço de arquivo do AFS a um volume. Ele age como um diretório padrão do UNIX no que se refere aos usuários poderem mudar de diretório e listar seu conteúdo com os comandos do UNIX **cd** e **ls**.

Proprietário de um Grupo. A pessoa ou grupo que pode administrar um grupo.

Quota. O limite de tamanho de um volume, atribuído pelo administrador do sistema e medido em blocos de kilobyte.

Senha. Uma cadeia de caracteres exclusiva definida pelo usuário que valida a identidade do sistema do usuário. O usuário deve fornecer a senha corretamente para que seja autenticado.

Servidor. Programa ou máquina que fornece um serviço especializado a seus clientes, como armazenamento e transferência de arquivos ou efetuação de autenticação.

Sinalizador. Parte de um comando que determina como o comando é executado, ou o tipo de saída que ele produz.

Sinalizador de Privacidade m. O terceiro sinalizador de privacidade em um grupo, que permite ao proprietário listar os membros de um grupo ou os grupos aos quais o usuário pertence.

Sinalizador de Privacidade o. O segundo sinalizador de privacidade em um grupo, que permite ao proprietário listar os grupos que pertencem ao usuário ou grupo.

Sinalizador de Privacidade r. O quinto sinalizador de privacidade em um grupo, que permite ao proprietário remover membros do mesmo.

Sinalizador de Privacidade s. O primeiro sinalizador de privacidade em um grupo, que permite ao proprietário listar informações gerais sobre ele.

Sinalizador Privado a. O quarto sinalizador privado em um grupo, que permite ao proprietário incluir membros no mesmo.

Sistema de Arquivos Distribuído. Um sistema de arquivos que une os sistemas de arquivos de máquinas individuais. Os arquivos são armazenados em máquinas diferentes na rede, mas podem ser acessados a partir de todas as máquinas.

Subdiretório. Diretório que se localiza em outro diretório na hierarquia de sistema de arquivos.

Taquigrafia do ACl all. Uma notação de taquigrafia utilizada com o comando **fs setacl** para representar todas as sete permissões.

Taquigrafia do ACL none. Uma notação de taquigrafia utilizada com o comando **fs setacl** para excluir uma entrada de um ACL.

Taquigrafia do ACL read. Uma notação de taquigrafia utilizada com o comando **fs setacl** para representar as permissões **r** e **l**.

Taquigrafia do ACL write. Uma notação de taquigrafia utilizada com o comando **fs setacl** para representar todas as permissões exceto a permissão **a**.

Token. Conjunto de dados que os processos do servidor do AFS aceita como evidência de que o proprietário comprovou com sucesso sua identidade para o serviço de autenticação do AFS da célula. O AFS atribui a identidade **anônima** aos usuários que não possuem um token.

Volume. Estrutura utilizada pelo AFS para agrupar um conjunto de arquivos e diretórios em uma única unidade para fins administrativos. O conteúdo de um volume se localiza em uma única partição de disco e deve ser instalado no espaço de arquivo do AFS para pode ser acessado.

Índice Remissivo

D

E

Q

R

S

T

U

V

Avisos

Primeira Edição (Abril de 2000)

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos E.U.A.

Pode ser que a IBM não ofereça em outros países os produtos, serviços ou recursos discutidos neste documento. Consulte o representante local da IBM para informar-se sobre produtos e serviços disponíveis em sua área. Qualquer referência nesta publicação a um produto, programa ou serviço licenciado IBM não determina ou implica que somente o produto, programa ou serviço licenciado pela IBM possa ser usado. Pode ser usado qualquer produto, programa ou serviço funcionalmente equivalente que não infrinja os direitos de propriedade intelectual da IBM. Cabe ao usuário, porém, a responsabilidade de avaliar e testar a operação de qualquer produto, programa ou serviço da IBM.

Pode ser que a IBM possua patentes ou pedidos pendentes de patente que tratam do assunto abordado neste documento. O fornecimento desta publicação não lhe garante nenhum direito sobre tais patentes. Dúvidas sobre licenças podem ser enviadas, por escrito, para:

Gerente de Relações Industriais e Comerciais da IBM
Av. Pasteur, 138/146
Botafogo - Rio de Janeiro
Brasil
Cep.: 22290-240

O parágrafo a seguir não se aplica ao Reino Unido ou a nenhum país em que tais disposições não estejam de acordo com a legislação local:

A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTE DOCUMENTO “NO ESTADO EM QUE ESTÁ” SEM GARANTIA DE ESPÉCIE ALGUMA, EXPLÍCITA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO AS GARANTIAS IMPLÍCITAS OU CONDIÇÕES DE NÃO-VIOLAÇÃO, DE COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM FIM ESPECÍFICO. Alguns estados não permitem renúncia a garantias explícitas ou implícitas em certas transações, motivo pelo qual essa declaração pode não aplicar-se ao seu caso.

Nestas informações pode haver imprecisões técnicas e erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições do documento. A IBM pode fazer melhorias

e/ou alterações no(s) produto(s) e/ou programa(s) descritos nesta publicação a qualquer momento, sem aviso prévio.

Quaisquer referências encontradas nestas informações aos sites Web não-IBM são fornecidas apenas por motivo de praticidade e de maneira alguma servem como endosso a tais sites Web. Os materiais desses sites Web não fazem parte dos materiais relativos a este produto IBM e o risco do uso desses sites Web deve ser assumido por quem se serve deles.

Ao enviar informações à IBM, ela pode utilizá-las ou distribui-las da forma como achar adequado sem que incorra em qualquer obrigação para com você.

Licenciados do programa que desejem obter informações a respeito dele a fim de permitir: (i) a troca de informações entre programas criados independentemente de outros programas (incluindo este) e (ii) o uso mútuo das informações que foram trocadas devem entrar em contato com o:

Centro de Atendimento a Clientes IBM
Av. Pasteur, 138/146
22290-240
Botafogo - RJ
Brasil.

Tais informações podem ser disponibilizadas mas estão sujeitas a prazos e condições vigentes, que podem incluir, em alguns casos, o pagamento de uma taxa.

O programa licenciado aqui descrito e todo o material licenciado disponível para ele são fornecidos pela IBM em conformidade com o Acordo para Licenças de Programas da IBM International ou com qualquer contrato equivalente celebrado entre ambas as partes.

Todos os dados sobre desempenho aqui contidos foram determinados em um ambiente controlado. Sendo assim, os resultados obtidos em outros ambientes operacionais podem variar significativamente. Algumas medidas podem ter sido tomadas em sistemas de nível de desenvolvimento e não há garantia de que estas medidas serão as mesmas nos sistemas geralmente disponíveis. Além disso, algumas medidas podem ter sido estimadas por extrapolação. Os resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

As informações relativas a produtos não-IBM foram obtidas dos fornecedores desses produtos, de propaganda publicada sobre eles ou de outras fontes de publicidade encontradas. A IBM não os testou e não pode confirmar a precisão de seu desempenho, sua compatibilidade nem qualquer outra alegação relacionada a produtos não-IBM. Dúvidas sobre os recursos de produtos não-IBM devem ser encaminhadas diretamente a seus fornecedores.

Todas as declarações que dizem respeito às intenções ou direção futura da IBM estão sujeitas a modificação e a cancelamento sem aviso prévio e representam apenas metas e objetivos.

Todos os preços da IBM são preços de revenda sugeridos pela IBM, atuais e sujeitos a alterações sem aviso prévio. Os preços dos revendedores podem variar.

Estas informações são apenas para fins de planejamento. Elas estão sujeitas a alterações antes que os produtos descritos tornem-se disponíveis.

São aqui fornecidos exemplos de dados e relatórios usados em operações de negócios do dia-a-dia. Para ilustrá-los da forma mais completa possível, os exemplos contêm nomes de usuários, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com nomes e endereços utilizados por uma empresa comercial real será mera coincidência.

Fotografias e ilustrações podem não aparecer na versão online destas informações.

Marcas

Os termos a seguir são marcas da International Business Machine Corporation nos Estados Unidos e em outros países:

AFS
AIX
AS/400
CICS
CICS OS/2
CICS/400
CICS/6000
CICS/ESA
CICS/MVS
CICS/VSE
CICSPlex
DB2
DCE Encina Lightweight Client
DFS
Encina
IBM
IMS
MQSeries
MVS/ESA
OS/2
OS/390
OS/400
PowerPC
RISC System/6000
RS/6000
S/390
Transarc
TXSeries
VSE/ESA
VTAM
VisualAge
WebSphere

Microsoft, Windows, Windows NT e o logotipo do Windows são marcas comerciais da Microsoft Corporation nos Estados Unidos e/ou em outros países.

Sun, SunLink, Solaris, SunOS, Java, todas as marcas e logotipos baseados em Java, NFS e Sun Microsystems são marcas ou marcas de serviço da Sun Microsystems, Inc. nos Estados Unidos e/ou outros países.

UNIX é uma marca de serviço nos Estados Unidos e em outros países licenciada exclusivamente através do X/Open Company Limited.

Outras empresas, produtos e nomes de serviços podem ser marcas ou marcas de serviço de outros.

Comentários do Leitor

AFS
Guia do Usuário

Publicação Nº G517-6974-00

Neste formulário, faça-nos saber sua opinião sobre este manual. Utilize-o se encontrar algum erro, ou se quiser externar qualquer opinião a respeito (tal como organização, assunto, aparência...) ou fazer sugestões para melhorá-lo.

Para pedir publicações extras, fazer perguntas ou tecer comentários sobre as funções de produtos ou sistemas IBM, fale com o seu representante IBM.

Quando você envia seus comentários, concede direitos, não exclusivos, à IBM para usá-los ou distribuí-los da maneira que achar conveniente, sem que isso implique em qualquer compromisso ou obrigação para com você.

Não se esqueça de preencher seu nome e seu endereço abaixo, se deseja resposta.

Comentários:

Nome

Companhia ou Empresa

Telefone

Endereço

Comentários do Leitor
G517-6974-00

Centro Industrial IBM do Brasil
Centro de Traduções
Caixa Postal, 70
13001-970 Campinas SP - Brasil.

Spine information:

AFS Guia do Usuário Versão 3.6 G517-6974-00